

PEARSON BENELUX BV

EN

.....

Verwerkersovereenkomst

DATUM.....('Ingangsdatum')

PARTIJEN:

Deze Verwerkersovereenkomst ('VWO') is een aanvulling op de gebruiksvoorwaarden die de Klant en Pearson zijn overeengekomen en maakt deel uit van het contract voor Diensten ('Hoofdovereenkomst') tussen

- (1) van('Klant')
- (2) Pearson Benelux BV, een besloten vennootschap met beperkte aansprakelijkheid naar Nederlands recht, geregistreerd bij de Kamer van Koophandel onder nummer 33215170 en kantoorhoudende aan de Kabelweg 37, 1014 BA Amsterdam, Nederland ('Pearson').

(samen de 'Partijen')

OVERWEGENDE DAT:

- A. De Klant vóór of op de Ingangsdatum één of meer Hoofdovereenkomsten heeft gesloten, waarmee toegang tot bepaalde diensten ('Diensten') van Pearson wordt gekocht.
- B. Vanaf de ingangsdatum deze VWO alle bepalingen die toezien op gegevensbescherming of Gegevensverwerking in elke Hoofdovereenkomst of eerdere verwerkersovereenkomst vervangt en deze overeenkomst in iedere Hoofdovereenkomst wordt opgenomen.
- C. De Klant optreedt als de Verwerkingsverantwoordelijke.
- D. Pearson optreedt als Verwerker.
- E. De Klant bepaalde Diensten zoals gedefinieerd in de Hoofdovereenkomst, die de Verwerking van Persoonsgegevens inhouden, wil uitbesteden aan Pearson.
- F. De Partijen een Verwerkersovereenkomst wensen te sluiten die voldoet aan de vereisten van het huidige wettelijke kader met betrekking tot gegevensverwerking en Verordening (EU) 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 het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).
- G. De Partijen hun rechten en verplichtingen willen vastleggen.

WORDT ALS VOLGT OVEREENGEKOMEN:

1. Definities en Interpretatie

- 1.1. Tenzij anders gedefinieerd hebben de begrippen en uitdrukkingen met een hoofdletter in deze Overeenkomst de volgende betekenis:
 - 1.1.1. '**Persoonsgegevens van de Klant**' betekent Persoonsgegevens die in de loop van de Diensten door Pearson als Verwerker of Sub-verwerker voor en namens de Klant worden verwerkt;
 - 1.1.2. '**Wetgeving op het gebied van Gegevensbescherming**' betekent de Europese wetgeving op het gebied van gegevensbescherming en, voor zover van toepassing, de wetgeving op het gebied van

gegevensbescherming of privacy van enig ander land. Deze definitie omvat ook alle amendementen, herzieningen of vervangingen van deze wetten en regels, evenals alle bindende besluiten of interpretaties van bevoegde autoriteiten, rechtbanken of toezichthoudende instanties voor gegevensbescherming;

- 1.1.3. **'AVG'** betekent de Algemene Verordening Gegevensbescherming 2016/679 van de EU;
- 1.1.4. **'Gegevensoverdracht'** betekent:
 - 1.1.4.1. een overdracht van Persoonsgegevens van de Klant aan Pearson; of
 - 1.1.4.2. een verdere overdracht van Persoonsgegevens van de Klant van Pearson naar een Sub-verwerker of tussen twee vestigingen van Pearson;
- 1.1.5. **'Beveiligingsincident'** betekent een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde openbaarmaking van of de ongeoorloofde toegang tot Persoonsgegevens van de Klant. Onder Beveiligingsincidenten vallen geen mislukte pogingen of activiteiten die de beveiliging van versleutelde Persoonsgegevens van de Klant niet in gevaar brengen;
- 1.1.6. **'Standaardbepalingen'** (of **'SSC's'**): de contractbepalingen in de bijlage bij Uitvoeringsbesluit 2021/914 van de Europese Commissie van 4 juni 2021 betreffende modelcontractbepalingen voor de overdracht van persoonsgegevens naar derde landen krachtens Verordening (EU) 2016/679 van het Europees Parlement en de Raad, zoals momenteel opgenomen in https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.
- 1.1.7. **'Sub-verwerker'** betekent een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat door of namens de Verwerker is aangesteld om namens de Klant Persoonsgegevens te verwerken met betrekking tot de Overeenkomst.
- 1.1.8. De termen **'Commissie'**, **'Verwerkingsverantwoordelijke'**, **'Betrokkene'**, **'Lidstaat'**, **'Persoonsgegevens'**, **'Inbreuk op persoonsgegevens'**, **'Verwerker'**, **'Verwerking'** en **'Toezichthoudende autoriteit'** hebben dezelfde betekenis als in de AVG en hun verwante termen worden dienovereenkomstig geïnterpreteerd.

2. Verwerkingsinstructies

- 2.1. Met het oog op de verstrekking door de Klant van Persoonsgegevens aan Pearson, stemt Pearson ermee in om de Persoonsgegevens van de Klant te verwerken overeenkomstig de voorwaarden en bepalingen van deze VWO en zoals uiteengezet in Bijlage 1 om de Hoofdovereenkomst uit te voeren.
- 2.2. Overeenkomstig artikel 2.3 erkennen en komen de Partijen overeen dat:
 - 2.2.1. Voor de doeleinden van deze VWO en tussen hen, is de Klant, of wordt de Klant beschouwd als, een Verwerkingsverantwoordelijke van Persoonsgegevens van de Klant en is Pearson, of wordt Pearson beschouwd als, een Verwerker of Sub-verwerker van Persoonsgegevens van de Klant;
 - 2.2.2. De Klant voldoet aan alle toepasselijke Wetgeving op het gebied van Gegevensbescherming en zijn/haar verplichtingen als Verwerkingsverantwoordelijke;
 - 2.2.3. Pearson voldoet aan alle toepasselijke Wetgeving op het gebied van Gegevensbescherming inzake de Verwerking van Persoonsgegevens van de Klant; en
 - 2.2.4. Pearson verwerkt geen Persoonsgegevens van de Klant anders dan op basis van de relevante gedocumenteerde instructies van de Klant, tenzij door toepasselijke wetgeving vereist.
- 2.3. Indien de Klant een Verwerker is, garandeert de Klant Pearson dat de instructies en handelingen van de Klant met betrekking tot de Persoonsgegevens van de Klant, met inbegrip van de benoeming van Pearson

als een andere Verwerker, door de relevante Verwerkingsverantwoordelijke zijn geautoriseerd en voldoen aan de toepasselijke Wetgeving op het gebied van Gegevensbescherming.

- 2.4. De Klant instrueert Pearson en Pearson stemt ermee in om de Persoonsgegevens van de Klant te verwerken om Diensten te leveren zoals uiteengezet in de Hoofdovereenkomst.

3. Personeel van Pearson

- 3.1. Pearson neemt redelijke stappen om de betrouwbaarheid te garanderen van elke werknemer, vertegenwoordiger of opdrachtnemer van Pearson die toegang heeft tot de Persoonsgegevens van de Klant, waarbij in elk afzonderlijk geval wordt gegarandeerd dat de toegang strikt beperkt wordt tot die personen die de relevante Persoonsgegevens van de Klant moeten kennen of er toegang tot nodig hebben, zoals strikt noodzakelijk is voor de doeleinden van de Hoofdovereenkomst, en om te voldoen aan de toepasselijke wetgeving in het kader van de taken van die persoon jegens Pearson.
- 3.2. Pearson garandeert dat alle personen die zij machtigt om Persoonsgegevens van de Klant te verwerken, onderworpen zijn aan verbintenissen inzake vertrouwelijkheid of professionele of wettelijke verplichtingen tot geheimhouding en alleen Persoonsgegevens van de Klant verwerkt zoals uiteengezet in deze VWO.

4. Rechten van de betrokkene

- 4.1. Rekening houdend met de aard van de Verwerking, helpt Pearson, voor zover mogelijk, de Klant door passende technische en organisatorische maatregelen door te voeren, om zo de verplichtingen van de Klant na te komen, zoals redelijkerwijs door de Klant begrepen, om te reageren op verzoeken om de rechten van Betrokkenen uit te oefenen op grond van de Wetgeving op het gebied van Gegevensbescherming.
- 4.2. Pearson:
 - 4.2.1. stelt de Klant onmiddellijk op de hoogte als er een verzoek van een Betrokkene wordt ontvangen op grond van een wet inzake de Wetgeving op het gebied van Gegevensbescherming met betrekking tot Persoonsgegevens van de Klant, en de Klant is verantwoordelijk voor de beantwoording van een dergelijk verzoek; en
 - 4.2.2. garandeert dat er niet op dat verzoek wordt gereageerd, behalve op grond van de gedocumenteerde instructies van de Klant of zoals vereist door de toepasselijke wetgeving waaraan Pearson is onderworpen, in welk geval Pearson, voor zover toegestaan door de toepasselijke wetgeving, de Klant informeert over die wettelijke vereiste voordat Pearson op het verzoek reageert.
- 4.3. Pearson verstrekt geen Persoonsgegevens van de Klant als reactie op een verzoek om toegang of openbaarmaking van een derde zonder voorafgaande schriftelijke toestemming van de Klant, behalve als hiertoe een verplichting bestaat overeenkomstig toepasselijke wetgeving of zoals anderszins toegestaan onder deze VWO of de Overeenkomst.

5. Beveiliging

- 5.1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, neemt Pearson met betrekking van Persoonsgegevens van de Klant passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen, dat passend is voor dat risico, met inbegrip van, in voorkomend geval, de maatregelen waarnaar wordt verwezen in artikel 32, lid 1, van de AVG.

- 5.2. Bij de bepaling van het passende beveiligingsniveau houdt Pearson vooral rekening met de risico's die de Verwerking met zich meebrengt, in het bijzonder door een Inbreuk op Persoonsgegevens.
- 5.3. De technische, beveiligings- en organisatorische maatregelen waarnaar in artikel 7.1 wordt verwezen, moeten minimaal voldoen aan de beveiligingseisen zoals uiteengezet in Bijlage 3.
- 5.4. De principes en aanbevelingen in ISO 27001, inclusief latere amendementen, moeten worden gebruikt als een kaderrichtsnoer om aan de eisen van de VWO te voldoen.

6. Beveiligingsincidenten

- 6.1. Pearson informeert de Klant over elk Beveiligingsincident waarvan zij kennis krijgt zonder onnodige vertraging en niet later dan 48 uur nadat zij kennis heeft gekregen van het Beveiligingsincident. Al deze kennisgevingen moeten worden gedaan overeenkomstig de mededelingsplichten zoals vastgelegd in deze VWO of naar goeddunken van Pearson door een telefoontje of e-mail naar de vertegenwoordiger van de Klant waarmee Pearson regelmatig contact onderhoudt.
- 6.2. Pearson neemt redelijke stappen om de gevolgen van Beveiligingsincidenten te verhelpen of beperken.
- 6.3. Pearson werkt met de Klant samen en verstrekt aan de Klant redelijke ondersteuning en informatie:
 - 6.3.1. bij het onderzoeken van Beveiligingsincidenten; en
 - 6.3.2. met betrekking tot kennisgevingen van een Beveiligingsincident die de Klant aan een toezichthouder doet.
- 6.4. Alle kosten die samenhangen met het afhandelen van een Beveiligingsincident en het nakomen van alle verplichtingen zijn voor rekening van de Klant als het Beveiligingsincident zich voordoet als gevolg van het niet nakomen door de Klant van de verplichtingen uit hoofde van deze VWO of het niet naleven van de gebruiksvoorwaarden van de Diensten door geautoriseerde gebruikers van de Klant.
- 6.5. De Klant is als enige verantwoordelijk voor de naleving van de wetgeving inzake het melden van incidenten met betrekking tot Persoonsgegevens van de Klant en het voldoen aan alle kennisgevingsverplichtingen jegens derden met betrekking tot Beveiligingsincidenten.
- 6.6. De kennisgeving van Pearson van of reactie op een Beveiligingsincident onder deze Clausule wordt niet opgevat als een erkenning door Pearson van enige fout of aansprakelijkheid met betrekking tot dat Beveiligingsincident.

7. Sub-verwerkers

- 7.1. Pearson geeft een entiteit van de Pearson-groep, Sub-verwerker of andere derde geen toegang tot de Persoonsgegevens van de Klant, maakt ze niet aan hen openbaar en schakelt hen ook niet in om deze te verwerken, tenzij:
 - 7.1.1. De Klant hiervoor vooraf uitdrukkelijk schriftelijke toestemming geeft;
 - 7.1.2. Pearson de entiteit van de Pearson-groep, de Sub-verwerker of andere derde voorwaarden oplegt die niet minder verplichtend zijn dan de voorwaarden die onder deze Overeenkomst aan Pearson worden opgelegd;
- 7.2. Niettegenstaande artikel 7.1 geldt het volgende vanaf de datum van deze Overeenkomst:
 - 7.2.1. De klant stemt in met de entiteiten van de Pearson-groep zoals opgenomen in Bijlage 2;

- 7.2.2. De Klant geeft toestemming voor de Sub-verwerkers zoals opgenomen in de bijgevoegde Bijlage 2 en de lijst van Sub-verwerkers op de website van Pearson op https://www.pearsonclinical.nl/platform_security_privacy; en
- 7.2.3. Pearson garandeert dat zij gegevensbeschermingsvoorwaarden heeft opgelegd aan de entiteiten van de Pearson-groep en de opgenomen Sub-verwerkers overeenkomstig 7.1.
- 7.3. Pearson moet de Klant op de hoogte stellen en specifieke schriftelijke goedkeuring van de Klant verkrijgen als Pearson een nieuwe Sub-verwerker in de arm wil nemen die momenteel niet in Bijlage 2 of op de website van Pearson vermeld staat. De kennisgeving moet ten minste 60 (zestig) dagen voordat Pearson de nieuwe Sub-verwerker in dienst wil stellen, zijn ontvangen.
- 7.4. Pearson blijft volledig aansprakelijk voor elke inbreuk op deze VWO die wordt veroorzaakt door een handeling, fout of nalatigheid van één van haar Sub-verwerkers die Persoonsgegevens van de Klant verwerken.

8. Gegevensbeschermingseffectbeoordelingen (DPIA) en Voorafgaande raadpleging

- 8.1. Pearson verleent redelijke bijstand aan de Klant met alle risicobeoordelingen, DPIA's aangaande gegevensbescherming en voorafgaand overleg met Toezichthoudende Autoriteiten of andere bevoegde autoriteiten voor gegevensbescherming, waarvan de Klant redelijkerwijs aanneemt dat deze vereist zijn op grond van artikel 32, 35 of 36 van de AVG of gelijkwaardige bepalingen van andere Wetgeving op het gebied van Gegevensbescherming, in elk geval uitsluitend met betrekking tot de Verwerking van Persoonsgegevens van de Klant door, en rekening houdend met de aard van de Verwerking en informatie die Pearson heeft.

9. Auditrechten

- 9.1. Op verzoek van de Klant, en niet vaker dan eenmaal per jaar, stelt Pearson alle redelijkerwijs passende informatie aan de Klant ter beschikking die nodig is om de naleving van de verplichtingen die zijn vastgelegd in deze VWO aan te tonen en staat Pearson audits toe en werkt hier aan mee, inclusief inspecties die worden uitgevoerd door de Klant of een andere auditor die door de Klant is gemachtigd.
- 9.2. Op verzoek van de Klant stelt Pearson de Klant gratis de documentatie van de Diensten ter beschikking die de beveiligings- en privacypraktijken van Pearson beschrijft, samen met relevante certificeringen, zoals ISO 27001 en het SOC 2-rapport. De Klant erkent dat Pearson door het verstrekken van deze documenten voldoet aan de controlevereisten zoals uiteengezet in artikel 28, lid 3, onder h) van de AVG of enige andere verplichting in een overeenkomst tussen de partijen met betrekking tot gegevensbescherming of informatiebeveiliging.
- 9.3. Als de Klant om verdere controle verzoekt, waaronder ook een audit of inspectie van de faciliteiten waar Pearson persoonsgegevens verwerkt, komen Pearson en de Klant de datum(s), de reikwijdte en de veiligheids- en vertrouwelijkheidscontroles overeen die van toepassing zijn op een dergelijke audit of inspectie.
- 9.4. Pearson kan een vergoeding voor een dergelijke audit of inspectie in rekening brengen zoals vastgelegd in artikel 9.3 en verstrekt de Klant voorafgaand aan een dergelijke audit of inspectie bijzonderheden over de toepasselijke vergoeding. De Klant is verantwoordelijk voor alle kosten in verband met een dergelijke audit of inspectie.

10. Internationale gegevensoverdrachten

10.1. Tijdens de uitvoering van de Diensten erkent de Klant dat Pearson en/of zijn Sub-verwerkers verwerkingsactiviteiten kunnen uitvoeren buiten het land van herkomst van de Persoonsgegevens van de Klant en dat de Persoonsgegevens van de Klant kunnen worden verzameld, verwerkt en/of opgeslagen in landen waar de toepasselijke wetgeving met betrekking tot de verwerking van Persoonsgegevens kan afwijken van die in het land van herkomst. Pearson garandeert dat dergelijke overdrachten worden uitgevoerd overeenkomstig goedgekeurde juridische mechanismen en met inachtneming van de vereisten van de toepasselijke Wetgeving op het gebied van Gegevensbescherming en deze VWO, met inbegrip van eventuele latere wettelijke amendementen of wetsontwerpen.

10.2. Als en voor zover de AVG van toepassing is op de Persoonsgegevens van de Klant die onderworpen zijn aan internationale gegevensoverdracht, draagt Pearson de Persoonsgegevens van de Klant alleen over aan ontvangers die over adequate waarborgen beschikken, waaronder mogelijk:

10.2.1. Een adequaatheidsbesluit van de Europese Commissie

10.2.2. SCC's goedgekeurd door de Europese Commissie

10.2.3. Bindende bedrijfsvoorschriften

11. Ingangsdatum en duur van de overeenkomst

11.1. De VWO gaat in op het moment dat deze door beide partijen is ondertekend.

11.2. De VWO is van kracht zolang de Verwerking van Persoonsgegevens wordt uitgevoerd en blijft van kracht totdat de verwerking wordt beëindigd.

11.3. De Klant geeft Pearson opdracht om de Persoonsgegevens van de Klant gedurende een redelijke periode na beëindiging of na afloop van de Hoofdovereenkomst te bewaren ter ondersteuning van eventuele latere controles of gegevensherstel die de Klant verlangt.

11.4. Daarna vernietigt of retourneert Pearson de Persoonsgegevens van de Klant die in haar bezit of onder haar controle zijn. De verplichting (om gegevens te vernietigen) is niet van toepassing voor zover Pearson door haar interne beleid of door een Uniewet (of een wet van een andere lidstaat van de Europese Unie) of enige andere toepasselijke wetgeving of door enige contractuele verbintenissen na beëindiging verplicht is om enkele of alle Persoonsgegevens van de Klant te bewaren. De bepalingen van deze VWO blijven van toepassing op alle Persoonsgegevens van de Klant die door Pearson worden bewaard, ongeacht beëindiging of afloop van de Hoofdovereenkomst.

11.5. Als Pearson of een Sub-verwerker failliet gaat, geliquideerd wordt of iets vergelijkbaars ondergaat en daarom stopt met het verwerken van Persoonsgegevens van de Klant, moeten alle Persoonsgegevens onmiddellijk zodanig aan de Klant worden teruggegeven dat de Klant ze kan blijven gebruiken. De Klant kan Persoonsgegevens ook rechtstreeks via het systeem exporteren en opslaan. Hierna is Pearson, de failliete boedel of vergelijkbaar, verplicht om de Persoonsgegevens overeenkomstig het bovenstaande uit haar systemen te verwijderen.

12. Gebruik van de-geïdentificeerde gegevens

12.1. De Klant komt overeen dat Pearson gedurende en na afloop van de Hoofdovereenkomst Persoonsgegevens van de Klant waaruit kenmerken zijn verwijderd die direct tot een individu herleidbaar zijn en die derhalve als geanonimiseerde gegevens worden beschouwd, mag gebruiken en openbaar mag maken voor benchmarking, educatief onderzoek, de ontwikkeling en verbetering van producten en

diensten of voor andere gerelateerde doeleinden. Dergelijke de-geïdentificeerde gegevens worden niet beschouwd als Persoonsgegevens van de Klant.

13. Vertrouwelijkheid

13.1. Elke Partij moet deze VWO en informatie die zij ontvangt over de Wederpartij en haar activiteiten in verband met deze VWO ('Vertrouwelijke Informatie') vertrouwelijk houden en mag deze Vertrouwelijke Informatie niet gebruiken of openbaar maken zonder voorafgaande schriftelijke toestemming van de Wederpartij, behalve voor zover:

13.1.1. openbaarmaking wettelijk verplicht is;

13.1.2. de informatie al openbaar is.

14. Kennisgevingen

14.1. Kennisgevingen in het kader van deze VWO worden schriftelijk gedaan en persoonlijk afgegeven, of via een koeriersdienst, een bevestigde e-mail of aangetekende post met ontvangstbevestiging, en worden geacht te zijn afgeleverd na persoonlijke afgifte, één (1) dag na afgifte door een koeriersdienst, na bevestiging van ontvangst van de e-mail of vijf (5) dagen na afgifte per post. Kennisgevingen worden naar het geregistreerde adres van een Partij gestuurd of een ander adres dat die Partij schriftelijk opgeeft.

15. Effect van amendement

15.1. Vanaf de Ingangsdatum vervangt deze gewijzigde VWO alle gegevensbeschermingsbepalingen in elke Hoofdovereenkomst en/of eerdere verwerkersovereenkomst en wordt deze opgenomen in elke Hoofdovereenkomst. In geval van strijdigheid of inconsistentie tussen de bepalingen van deze VWO en de rest van de toepasselijke Hoofdovereenkomst, gelden de voorwaarden van deze VWO. Onder voorbehoud van de amendementen in deze VWO blijft elke Hoofdovereenkomst onverminderd van kracht. Voor de duidelijkheid: als de Klant meer dan één Hoofdovereenkomst is aangegaan, wijzigt deze VWO elk van de Hoofdovereenkomsten afzonderlijk.

GETEKEND voor en namens de Klant

Handtekening

Naam

Functie

GETEKEND voor en namens Pearson Benelux B.V

Handtekening

Gert Jaap Schoppink

Gert Jaap Schoppink (May 2, 2024 08:30 GMT+1)

Naam

Gert Jaap Schoppink

Functie

Managing Director

Bijlage 1 – Instructies voor de Gegevensverwerker

1. Instructies

- 1.1. De Klant geeft Pearson hierbij opdracht om de Persoonsgegevens van de Klant te verwerken om Diensten te verrichten zoals uiteengezet in de Hoofdovereenkomst.
- 1.2. Als Pearson de verwerking van de Persoonsgegevens van de Klant toevertrouwt aan Sub-verwerkers, zoals goedgekeurd in Bijlage 2, is Pearson verantwoordelijk voor het aangaan van schriftelijke overeenkomsten met hen, waarin voorwaarden zijn opgenomen in overeenstemming met deze VWO.

2. Doel van de verwerking

- 2.1.1. De verwerking van de Persoonsgegevens van de Klant wordt uitgevoerd voor de volgende specifieke doeleinden: om de levering van het klinische beoordelingssysteem te vergemakkelijken, zodat de Klant klinische beoordelingen kan uitvoeren zoals beschreven in de Hoofdovereenkomst.
- 2.1.2. Klantenondersteuning en technische ondersteuning bieden met betrekking tot het gebruik van het klinische beoordelingssysteem.
- 2.2. Pearson verwerkt de Persoonsgegevens van de Klant overeenkomstig deze gespecificeerde doeleinden en eventuele verdere instructies van de Klant.
- 2.3. Pearson mag de Persoonsgegevens van de Klant niet voor andere doeleinden gebruiken.
- 2.4. De Persoonsgegevens van de Klant mogen niet worden verwerkt volgens andere instructies dan die van de Klant.

3. Algemene beschrijving van de verwerking

Q-interactive

- 3.1. Het testen wordt gedaan met twee iPads in een app met de naam Assess. De testleider gebruikt de eerste iPad om toegang te krijgen tot de instructies voor het afnemen van de test, om antwoorden te scoren en te registreren en om visuele stimuli te bedienen. De kandidaat gebruikt de andere iPad om stimuli te bekijken en erop te reageren.
- 3.2. Q-interactive bestaat ook uit een website die wordt gebruikt om rapporten te genereren voor afnames die zijn gedaan op de iPads en om gegevens voor de lange termijn op te slaan.
- 3.3. De testafnemer kan nieuwe gebruikers aanmaken, licenties aan hen toewijzen, het verbruik in het account bijhouden en testgegevens van alle kandidaten in het account bekijken.
- 3.4. Binnen Q-interactive is er ook een rol als Beheerder Assistent. De beheerder assistent kan gebruikers aanmaken, licenties aan hen toewijzen en het verbruik bijhouden, maar ze kunnen geen testgegevens van kandidaten inzien.

Q-global

- 3.5. Met een website kunnen nieuwe kandidaten worden aangemaakt en handmatig gegevens van een afgenomen test worden geregistreerd om een digitaal rapport te verkrijgen dat lokaal opgeslagen en/of afgedrukt kan worden.

4. Soorten persoonsgegevens

De verwerking omvat persoonsgegevens van de hieronder aangekruiste categorieën.

Persoonsgegevens

- | | |
|--|---|
| <input checked="" type="checkbox"/> Naam | <input type="checkbox"/> ID-documenten (zoals paspoort of rijbewijs) |
| <input checked="" type="checkbox"/> Geboortedatum | <input type="checkbox"/> Financiële informatie |
| <input checked="" type="checkbox"/> E-mailadres | <input type="checkbox"/> Accountgegevens van sociale media |
| <input checked="" type="checkbox"/> Telefoonnummer | <input type="checkbox"/> Arbeidsverleden en werkgerelateerde informatie |
| <input type="checkbox"/> Postadres | <input type="checkbox"/> Onderwijs en studieverloop |
| <input type="checkbox"/> Nationaal identificatienummer | |

Speciale categorieën persoonsgegevens

- | | |
|---|---|
| <input checked="" type="checkbox"/> Ras of etnische afkomst | <input type="checkbox"/> Vakbondslidmaatschap |
| <input type="checkbox"/> Politieke overtuiging | <input checked="" type="checkbox"/> Gegevens over gezondheid |
| <input type="checkbox"/> Geloofsovertuiging | <input type="checkbox"/> Gegevens over seksleven of seksuele geaardheid |
| <input type="checkbox"/> Levensbeschouwelijke overtuiging | |

5. Categorieën van betrokkenen

5.1. Er worden gegevens over de volgende categorieën van betrokkenen verwerkt:

- 5.1.1. Een Aanbieder/Testleider van onderzoeken, zoals een psycholoog of andere zorgverlener.
- 5.1.2. Een patiënt/kandidaat die via Q-interactive door een psycholoog of andere zorgverlener wordt onderzocht.

6. Derde landen (niet-EU-lidstaten)

6.1. Pearson kan aan de volgende derde landen persoonsgegevens doorgeven:

6.1.1. Canada

6.2. Met betrekking tot Canadese particuliere bedrijven wordt er door het adequaatheidsbesluit van 2001 van de EU-Commissie een adequaat beschermingsniveau gegarandeerd.

Bijlage 2 – Sub-verwerkers van Pearson

Pearson gebruikt de volgende Sub-verwerker(s) met betrekking tot de taken die Pearson voor de Klant uitvoert. Door het aangaan van de VVO stemt de Klant in met het gebruik van deze Sub-verwerker(s).

Eén tabel per sub-verwerker.

	Bedrijfsnaam	Reg. nr.	Adres	Beschrijving van de verwerking	Redenen voor overdracht
Subgegevensverwerker (1. Niveau)	Amazon Web Services Canada, Inc.	857305932	120 Bremner Blvd, 27 ^{ste} verdieping, Toronto, ON, M5J 0A8, Canada	Cloudcomputing-diensten en datacenteractiviteiten. Hosten van persoonsgegevens van klanten. Ondersteuning op initiatief van de klant. Uitsluitend toegang tot gegevens na de uitdrukkelijke toestemming van de Klant op het moment van het verzoek.	Adequaatheidsbesluit van de Europese Unie
Subgegevensverwerker (2. Niveau)	Amazon Data Services Canada, Inc.	797963121	160 Elgin Street Suite 2600, Ottawa, ON, K1P 1C3	Cloudcomputing-diensten en datacenteractiviteiten. Hosten van Persoonsgegevens van Klanten.	Adequaatheidsbesluit van de Europese Unie

	Bedrijfsnaam	Reg. nr.	Adres	Beschrijving van de verwerking	Redenen voor overdracht
Subgegevensverwerker (1. Niveau)	Bahnhof	831671	Sveavagen 41, 111 40 Stockholm, Zweden	Hosten van Persoonsgegevens van Klanten.	N.v.t.
Subgegevensverwerker (2. Niveau)	Geen				

	Bedrijfsnaam	Reg. nr.	Adres	Beschrijving van de verwerking	Redenen voor overdracht
Subgegevensverwerker (1. Niveau)	SendGrid van Twilio (Twilio Ireland Limited)	IE557454	3 Dublin Landings, North Wall Quay, Dublin 1, Ierland	Routing en verzending van e-mails. Persoonsgegevens in e-mails worden naar de doel-e-mail verzonden. De gegevens in de hoofdtekst van de e-mail worden niet langer bewaard dan nodig is om de e-mail te versturen. Het doel-e-mailadres wordt bewaard voor analytische doeleinden.	Adequaathheidsbesluit van de Europese Unie – Kader voor gegevensbescherming
Subgegevensverwerker (2. Niveau)	AWS Amazon USA	0000174230	410 Terry Avenue North, Seattle, WA 98109-5210, VS.	Hosting van SendGrid-gegevens.	Adequaathheidsbesluit van de Europese Unie – Kader voor gegevensbescherming

	Bedrijfsnaam	Reg. nr.	Adres	Beschrijving van de verwerking	Redenen voor overdracht
Subgegevensverwerker (1. Niveau)	MongoDB Atlas (MongoDB Limited)	4999921	Building Two, Number One Ballsbridge, Shellbourne Road, Dublin 4, Co Dublin, Ierland	Database as a service voor het hosten van persoonsgegevens van klanten.	N.v.t.
Subgegevensverwerker (2. Niveau)	Amazon Web Services Canada, Inc.	857305932	120 Bremner Blvd, 27 ^{ste} verdieping, Toronto, ON, M5J 0A8, Canada	Hosten van MongoDB Atlas-gegevens.	Adequaathheidsbesluit van de Europese Unie

	Bedrijfsnaam	Reg. nr.	Adres	Beschrijving van de verwerking	Redenen voor overdracht
Subgegevensverwerker (entiteit van de Pearson-groep)	Pearson Education Limited (Verenigd Koninkrijk)	872828	80 Strand, Londen, WC2R 0RL, Verenigd Koninkrijk	Klantenondersteuning. Uitsluitend toegang tot cliënt/afnamegegevens na uitdrukkelijke toestemming van de klant op het moment van het verzoek.	Adequaatheidsbesluit van de Europese Unie Alle Pearson-entiteiten zijn gebonden door onze intercompany <i>International Data Transfer Agreement</i> (IDTA; Internationale Gegevensoverdrachtsovereenkomst)
Subgegevensverwerker (entiteit van de Pearson-groep)	Pearson Canada Assessment Inc. (Canada)	1163650766	176 Yonge Street, 7 ^{de} verdieping, Toronto, ON, M5C 2L7, Canada	Technische ondersteuning.	Adequaatheidsbesluit van de Europese Unie Alle Pearson-entiteiten zijn gebonden door onze intercompany <i>International Data Transfer Agreement</i> (IDTA; Internationale Gegevensoverdrachtsovereenkomst)
Subgegevensverwerker (entiteit van de Pearson-groep)	NCS Pearson, Inc (VS)	410850527	5601 Green Valley Drive, Bloomington, MN 55437, Verenigde Staten	Derdelijns technische ondersteuning. Uitsluitend toegang tot cliënt/afnamegegevens na uitdrukkelijke toestemming van de klant op het moment van het verzoek.	Alle Pearson-entiteiten zijn gebonden door onze intercompany <i>International Data Transfer Agreement</i> (IDTA; Internationale Gegevensoverdrachtsovereenkomst)

Ga voor een volledige lijst van Sub-verwerkers naar

https://www.pearsonclinical.nl/platform_security_privacy

Bijlage 3 – Informatiebeveiligingseisen

1. Algemene beveiligingseisen. Pearson:

- 1.1. Voldoet aan toepasselijke overheidswetgeving en door de branche opgelegde informatiebeveiligingsstandaarden (voorbeelden van dergelijke standaarden zijn onder andere ISO/IEC 27001, de *Payment Card Industry-Data Security Standards* (PCI-DSS), EDI-standaarden (*Electronic Data Interchange*) en de informatiebeveiligingseisen die zijn vastgelegd in wetten, zoals de *Health Insurance Portability and Accountability Act* – HIPAA).
- 1.2. Zet een formeel en uitgebreid beveiligingsprogramma op en onderhoudt dit overeenkomstig de beste industriële praktijk met redelijke en passende administratieve, organisatorische, technische en fysieke beveiligingen, met inbegrip van die welke zijn opgenomen in deze Bijlage 3 (de 'Informatiebeveiligingseisen'), die zijn ontworpen om de vertrouwelijkheid, integriteit en beschikbaarheid van Persoonsgegevens van de Klant te waarborgen (waaronder, maar niet beperkt tot, de privacy van Persoonsgegevens van de Klant) en om bescherming te bieden tegen Beveiligingsincidenten. Dergelijke gegevensbeveiligingen omvatten, maar zijn niet beperkt tot, het volgende:
 - 1.2.1. Pearson houdt een overzicht bij van de systemen die Pearson gebruikt om de Persoonsgegevens van de Klant op te slaan of te verwerken;
 - 1.2.2. Alle papieren materialen met Persoonsgegevens van de Klant of gerelateerde applicatie ondersteuning worden beveiligd in afgesloten houders als ze niet worden gebruikt en middels veilige versnippering op elk moment tijdens of aan het einde van de looptijd van deze VWO of op verzoek van de Klant vernietigd. De Klant kan om één of meer certificaten van vernietiging verzoeken;
 - 1.2.3. Het isoleren van Klantgegevens van gegevens en informatie van andere klanten en van Pearson zelf;
 - 1.2.4. Zorgen voor gedocumenteerde procedures voor veilige back-up en herstel van de Persoonsgegevens van de Klant, die minimaal sterke encryptie, veilige procedures voor het transport, de opslag en de verwijdering van de back-ups van de Persoonsgegevens van de Klant omvatten, met een gedocumenteerde "chain of custody".
 - 1.2.5. Gebruik van sterke encryptie om Persoonsgegevens bij verzending en opslag te beschermen.

2. Betrouwbaarheid van personeel

- 2.1. Indien wettelijk toegestaan, voert Pearson een uitgebreid achtergrondonderzoek uit naar alle werknemers voordat zij toegang verleent tot de Persoonsgegevens van de Klant, waaronder de verificatie van de identiteit, het adres, de arbeidsgeschiedenis/geschiktheid en beroepskwalificaties van elk teamlid van Pearson, naast aanvullende controles zoals een screening op drugsgebruik en een evt. strafblad (indien beschikbaar);
- 2.2. Pearson voert een formeel beleid met betrekking tot de voorwaarden en tijdlijnen voor toegang tot systemen van de Klant of van Pearson aan personen die toetreden of personen die in een andere rol gaan werken, en intrekking voor personen die om welke reden dan ook vertrekken.
- 2.3. Pearson garandeert dat alle bevoegde personen relevante, redelijke en noodzakelijke opleiding en ervaring hebben.
- 2.4. Pearson garandeert dat alle bevoegde personen die met Persoonsgegevens van de Klant omgaan op de hoogte zijn van de vertrouwelijke aard van de Persoonsgegevens van de Klant en een passende opleiding hebben gevolgd met betrekking tot hun verplichtingen in verband met de omgang met die gegevens, waaronder toepasselijke wet- en regelgeving, mogelijke verplichtingen inzake beveiliging of melding van inbreuken en aanvaardbaar gebruik van en de juiste procedures voor het opslaan en verzenden van

Persoonsgegevens van de Klant. Pearson houdt de gegevens van deze opleiding bij en stelt ze op verzoek beschikbaar aan de Klant.

3. Systeembeveiliging. Pearson:

- 3.1. Voldoet waar van toepassing aan het gedeelde beveiligingsmodel van hun Cloud Hosting Provider en de best practices, zoals beschreven door de Cloud Security Alliance, Cloud Control Matrix.
- 3.2. Beschermt Persoonsgegevens van de Klant door informatiebronnen zodanig te implementeren dat ze logisch gesegmenteerd zijn op basis van de gelijksoortigheid van het doel en zorgt ervoor dat elk segment is gescheiden en wordt beschermd via apparaten en diensten (zoals web- en netwerkbeveiligingsgateways, firewalls, etc.) die zijn geconfigureerd en beveiligd om te fungeren als beveiligingspunten.
- 3.3. Gebruikt in alle gevallen Sterke Encryptie (zoals FIPS 197) om Persoonsgegevens van de Klant te beschermen tijdens de overdracht of in rust.
- 3.4. Zet waar van toepassing netwerk- of cloudbeschermingscontroles in die schadelijk verkeer dat de informatiebronnen van Pearson binnenkomt of verlaat, kunnen opsporen en blokkeren.
- 3.5. Verwijdert Persoonsgegevens van de Klant alleen uit hun onmiddellijke controle als dit schriftelijk door de Klant is gemachtigd. Indien daartoe gemachtigd (bijv. in verband met offsite opslag van gegevensback-ups), mogen dergelijke Persoonsgegevens van de Klant alleen worden overgebracht op apparaten die zijn geconfigureerd met volledige schijfencryptie om de gegevens tegen verlies of diefstal te beschermen.
- 3.6. Slaat Persoonsgegevens van de Klant niet op verwisselbare media op (zoals USB-sticks, geheugensticks, tapes, cd's of externe harde schijven), behalve: (a) voor back-ups, bedrijfscontinuïteit, noodherstel en gegevensuitwisselingsdoeleinden zoals toegestaan en vereist onder deze VWO, en (b) in alle gevallen met gebruik van Sterke Encryptie.
- 3.7. Zorgt ervoor dat alle Informatiebronnen van Pearson 'gehard' zijn en blijven overeenkomstig het "*centre for internet security hardening benchmark*" (<https://www.cisecurity.org/>) en/of door de leverancier geleverde beveiligingsgids.

4. Security Gateways. Pearson:

- 4.1. Vereist een Sterke Authenticatie voor administratieve en/of managementtoegang tot Security Gateways, inclusief toegang om logbestanden te bekijken.
- 4.2. Heeft en gebruikt gedocumenteerde controles, beleid, processen en procedures om te garanderen dat onbevoegde gebruikers geen administratieve en/of managementtoegang hebben tot Security Gateways en dat gebruikersautorisatieniveaus voor het beheren en managen van Security Gateways passend zijn.
- 4.3. Garandeert dat Security Gateway-configuraties minimaal eens in de zes (6) maanden worden gehard door een steekproef van Security Gateways te selecteren en te controleren of elke standaardregelset en set configuratieparameters is geïmplementeerd.
- 4.4. Gebruikt bewakingsinstrumenten om te valideren dat alle aspecten van Security Gateways (zoals hardware, firmware en software) continu operationeel zijn.
- 4.5. Configureert en implementeert alle Security Gateways zodanig dat alle niet-operationele Security Gateways alle toegang weigeren.
- 4.6. Configureert real-time waarschuwingen voor wijzigingen in de configuratie en/of regelbasis van de Security Gateway.

5. Identificatie en Authenticatie.

- 5.1. Met betrekking tot toegang tot Persoonsgegevens van de Klant, hetzij in elektronische vorm of op papier, door het team van Pearson, zal Pearson:
 - 5.1.1. Sterke authenticatie vereisen (d.w.z. multifactorauthenticatie) voor elk gebruik van niet-openbare Informatiebronnen op afstand.
 - 5.1.2. Garanderen dat toegang tot systemen die Persoonsgegevens van de Klant verwerken, wordt afgedwongen via een gecentraliseerde identiteitsprovider die voldoet aan de *best practices* binnen de sector.
 - 5.1.3. Een veilige methode gebruiken voor de overdracht van authenticatiegegevens (zoals wachtwoorden) en authenticatiemechanismen (zoals tokens of smartcards).
 - 5.1.4. Waar nodig een op risico gebaseerd authenticatiemechanisme gebruiken, zodat de authenticatiemethoden gefaseerd zijn en in verhouding staan tot de gevoeligheid van Persoonsgegevens van de Klant waartoe toegang wordt verkregen (d.w.z. het gebruik van sterkere vormen van authenticatie voor toegang tot Persoonsgegevens van Klanten).
 - 5.1.5. Beschikken over en gebruikmaken van een gedocumenteerd proces voor het levenscyclusmanagement van gebruikers-ID's, inclusief procedures voor het goedkeuren van het aanmaken van accounts, het verwijderen van accounts onmiddellijk na beëindiging of binnen 24 uur na wijziging van de rol en het wijzigen van accounts (d.w.z. wijzigingen in privileges, toegangsbereik, functies/rollen) voor alle informatiebronnen en in alle omgevingen (zoals productie, test, ontwikkeling, enz.). Dergelijke processen omvatten een beoordeling van de toegangsprivileges en de geldigheid van accounts die ten minste elk kwartaal wordt uitgevoerd.

6. Software en gegevensintegriteit. Pearson:

- 6.1. Garandeert dat haar computer-, netwerk- en opslagbronnen zijn geconfigureerd om gebruik te maken van beveiligingsmogelijkheden die de uitvoering van kwaadaardige code detecteren, in quarantaine plaatsen en voorkomen.
- 6.2. Scheidt niet-productie Informatiebronnen van productie Informatiebronnen met behulp van computer-, netwerk- en opslagbronnen.
- 6.3. Gebruikt alleen gemaskeerde gegevens in ontwikkel- en testomgevingen. Als dit niet mogelijk is, heeft Pearson de schriftelijke toestemming van de Klant nodig om niet-de-geïdentificeerde Persoonsgegevens van Klanten te gebruiken en Pearson garandeert en verbindt zich ertoe dat dergelijke omgevingen toegangscodes hebben die even streng zijn als die welke in de productie worden gebruikt.
- 6.4. Beschikt over een gedocumenteerd wijzigingsbeheerproces, inclusief beoordeling van de gevolgen voor de beveiliging en back-upprocedures voor alle productieomgevingen.
- 6.5. Voor toepassingen die gebruikmaken van een database die wijzigingen in de Persoonsgegevens van de Klant mogelijk maakt, schakelt Pearson functies in voor het loggen van databasetransacties en bewaart Pearson de databasetransactielogs minimaal twaalf (12) maanden.
- 6.6. Controleert deze software om alle beveiligingskwetsbaarheden te vinden en verhelpen (statische, dynamische en afhankelijkheidscodeanalyse) voorafgaand aan de eerste implementatie en bij alle wijzigingen en updates van alle software die onder een VWO met Pearson is ontwikkeld.
- 6.7. Voert kwaliteitsborgingstesten uit (met een CREST en/of CHECK geaccrediteerde beveiligingsbeoordelaar) voor de beveiligingscomponenten (bijv. testen van identificatie, authenticatie, autorisatie, vertrouwelijkheid, integriteit, beschikbaarheid, functies voor onweerlegbaarheid) en alle andere

activiteiten die zijn ontworpen om de beveiligingsarchitectuur te valideren tijdens de eerste implementatie en bij alle wijzigingen en updates.

7. Kwetsbaarheden scannen en penetratietesten. Tijdens de looptijd van deze VWO of zolang Persoonsgegevens van de Klant door Pearson worden verwerkt (naargelang welke later is), zal Pearson:
 - 7.1. Gebruikmaken van standaardhulpmiddelen en handmatige technieken om de beveiliging van de door Pearson geleverde oplossing(en) te beoordelen.
 - 7.2. Ten minste elk kwartaal en onmiddellijk na elke belangrijke wijziging en upgrade een kwetsbaarheidsscan uitvoeren op extern en intern gerichte Informatiebronnen, waaronder netwerken, servers, toepassingen en databases, met toepasselijke software voor het scannen van standaardbeveiligingskwetsbaarheden om beveiligingskwetsbaarheden aan het licht te brengen en ervoor te zorgen dat dergelijke Informatiebronnen op de juiste manier worden beveiligd.
 - 7.3. Minimaal elk kwartaal testen of er ongeautoriseerde draadloze netwerken zijn.
 - 7.4. Minimaal eenmaal per jaar penetratietests laten uitvoeren door een derde, die op verzoek via screenshare worden gedeeld. Als er via deze tests kwetsbaarheden worden geïdentificeerd, biedt Pearson tijdig voldoende technisch personeel en ondersteuning om de geïdentificeerde problemen op te lossen en door te gaan met het uitvoeren van verdere ethische hacks totdat de Klant ervan verzekerd is dat de geïdentificeerde incidenten en hun onderliggende oorzaken zijn verholpen.
8. Loggen. Pearson:
 - 8.1. Registreert geprivilegieerde accounts op alle apparaten en applicaties.
 - 8.2. Registreert toegang tot gegevens (lezen), schrijven, wijzigen en pogingen tot aanmelden, mislukte toegangspogingen, wijzigingen in toegangscontrolelijsten, identifiers of groeps-/rolprivileges, updates van beveiligingssoftware of de functionaliteit van software en applicaties en de uitvoering van programma's die toegangscontroles kunnen omzeilen.
 - 8.3. Implementeert een real-time logserver en beperkt de toegang tot beveiligingslogs tot bevoegde personen en beschermt beveiligingslogs tegen ongeautoriseerde wijzigingen en een gecentraliseerde manier om beveiligingslogs te controleren. Alle beveiligings- en beveiligingsgerelateerde auditlogs voor anomalieën moeten minimaal wekelijks worden gecontroleerd en alle gelogde beveiligingsproblemen moeten tijdig worden opgelost.
 - 8.4. Bewaart alle beveiligings- en serverlogs gedurende een periode van één jaar (waarvan 90 dagen online beschikbaar) of zoals vereist om te voldoen aan wettelijke vereisten, naargelang welke periode het langst is. Het log registreert alle logische toegangspogingen, zowel geldige als ongeldige. Het log bevat de naam (ID), datum en tijd van het inloggen, de geraadpleegde records en de uitgevoerde activiteit. Indien mogelijk bevat het log ook een vermelding voor uitloggen.
9. Fysieke beveiliging. Pearson:
 - 9.1. Garandeert dat alle systemen die worden gebruikt om Persoonsgegevens van de Klant te verwerken en op te slaan, zich in veilige, bewaakte en toegangsgecontroleerde ruimten bevinden;
 - 9.2. Brengt alle Informatiebronnen onder in beveiligde faciliteiten met toegang die is beperkt tot bevoegde personen;
 - 9.3. Brengt alle Informatiebronnen onder op plaatsen die een adequaat juridisch kader bieden om naleving van de voorwaarden van deze VWO te waarborgen;

9.4. Bewaakt en registreert, voor auditdoeleinden, de toegang tot de fysieke faciliteiten waar Informatiebronnen staan die bedoeld zijn voor gebruik door meerdere gebruikers, inclusief de naam van de medewerker, tijd en datum van binnenkomst en vertrek, en bewaakt waar mogelijk de ruimte met een camera.

10. Mobiele en Draagbare apparaten. Pearson:

10.1. Evalueert minimaal eens per jaar het gebruik van en de controles voor alle door Pearson beheerde Mobiele en Draagbare apparaten om ervoor te zorgen dat de Mobiele en Draagbare apparaten kunnen voldoen aan de toepasselijke Informatiebeveiligingseisen.

10.2. Draadloze netwerken. Indien schriftelijk door de Klant goedgekeurd garandeert Pearson bij het gebruik van draadloze netwerktechnologieën op basis van radiofrequentie (RF) om Diensten voor de Klant uit te voeren of te ondersteunen dat alle Persoonsgegevens van de Klant die worden verzonden, worden beschermd door het gebruik van passende encryptietechnologieën die voldoende zijn om de vertrouwelijkheid van de Persoonsgegevens van Klanten te beschermen. Het gebruik van op RF gebaseerde draadloze headsets, toetsenborden, microfoons en aanwijsapparaten, zoals muizen, touchpads en digitale tekentabletten, vallen niet onder deze vereiste.