

Privacy procedures: Q-global & Q-interactive

Dit whitepaper: (a) is alleen bedoeld voor informatieve doeleinden, (b) vertegenwoordigt het huidige productaanbod en de huidige procedures van Pearson Clinical, die zonder voorafgaande kennisgeving kunnen worden gewijzigd. Pearson overeenkomsten regelen de verantwoordelijkheden en aansprakelijkheden van Pearson ten opzichte van zijn klanten, en dit document maakt geen deel uit van, noch wijzigt het, enige overeenkomst tussen Pearson en zijn klanten. Bovendien bevat dit document geen juridisch advies en de informatie in dit document houdt mogelijk geen rekening met toekomstige wijzigingen in wet- en regelgeving. We dringen er bij klanten op aan om hun juridisch adviseur te raadplegen om vertrouwd te raken met de vereisten die van toepassing zijn op hun specifieke situatie en om een onafhankelijke beoordeling te kunnen maken van de informatie in dit whitepaper.

Introductie

Pearson neemt gegevensbescherming en privacy serieus en integreert deze componenten als fundamentele principes in het kader van de ontwikkeling van producten en diensten. Dit whitepaper heeft als doel de privacy- en beveiligingsmaatregelen, die Pearson heeft geïmplementeerd voor Q-global en Q-interactive, te verduidelijken. Q-global en Q-interactive zijn web gebaseerde platformen, gericht op het betrouwbaar afnemen, scoren en rapporteren van tests. Gezien het grote belang van de bescherming van de persoonsgegevens van klanten (zoals gedefinieerd in de relevante wetgeving inzake gegevensbescherming), benadrukt dit document, samen met de **Gebruiksvoorwaarden** en het **Privacybeleid** van Pearson, de toewijding van Pearson aan de bescherming van de persoonsgegevens van klanten. Pearson bereikt dit door middel van strikte protocollen met betrekking tot het verzamelen, verwerken, opslaan en beveiligen van gegevens, in strikte overeenstemming met de toepasselijke wet- en regelgeving op het gebied van gegevensbescherming.

Overzicht van Q-global en Q-interactive

Beide platformen van Pearson worden gebruikt door specialisten in de geestelijke gezondheidszorg, docenten en andere professionals om tests af te nemen, scores te berekenen en efficiënt rapporten te genereren. De systemen zijn op elk moment toegankelijk vanaf elke computer en bevatten meer dan 60 toonaangevende meetinstrumenten. Alle functies van deze platformen werken binnen een veilige, besloten web omgeving en helpen professionals bij het stroomlijnen van hun afnameprocedures.

Gegevensverzameling en -verwerking

De onderstaande tabel geeft een overzicht van de soorten persoonsgegevens die binnen Q-global en Q-interactive verzameld worden en de doeleinden voor elke categorie:

Categorieën van betrokkenen	Categorieën van verzamelde persoonsgegevens	Doel van de verzameling
Patiënt/kandidaat	Naam (optioneel)	Identificatie van de patiënt
	Geboortedatum	Het berekenen van de testleeftijd van de patiënt en draagt bij aan een juiste afname en scoring
	ID (optioneel)	Identificatie van de patiënt
	Demografische gegevens	Voor de administratie van de afname en extra informatie in het scorerapport
	Responses tijdens de afname	Antwoorden van de patiënt op testitems zijn nodig om te kunnen scoren
	Scores	Berekende scores voor rapportage/verslaglegging
Aanbieder, Testleider	Gebruikersnaam	Toegang verlenen tot het platform
	Naam	Identificatie van de klant
	E-mail	Om de ontvangst van systeem e-mails mogelijk te maken
	Telefoonnummers	Om contact op te kunnen nemen bij technische problemen en de ondersteuning daarbij

De minimalisatie van gegevens is een fundamenteel principe in onze aanpak van dataprivacy en gegevensbescherming. Als leveranciers van klinische producten geven we prioriteit aan het verzamelen van alleen die gegevens die essentieel zijn voor het afnemen van tests, waarbij

privacy en naleving van de regelgeving worden gewaarborgd. Daarnaast bieden we optionele gegevensvelden aan, om zo onze klanten in staat te stellen zelf de controle te kunnen uitoefenen over de gegevensverwerking en om een vertrouwensrelatie op te bouwen.

Wettelijke basis en rol van Pearson met betrekking tot de Pearson

Clinical platformen:

De digitale platformen van Pearson Clinical beheren verschillende soorten persoonsgegevens van klanten en daarom wisselt de rol van Pearson bij het verwerken van persoonsgegevens afhankelijk van de bron en het doel.

- 1. Gegevens van docenten, gekwalificeerde klanten en testleiders:** In gevallen waarin er binnen de platformen van Pearson Clinical persoonsgegevens verwerkt worden die door deze partijen worden verstrekt, treedt Pearson op als gegevensverwerker. Pearson verwerkt persoonsgegevens op basis van de instructies van de klant, die op zijn beurt optreedt als verwerkingsverantwoordelijke, en zorgt voor de naleving van zijn richtlijnen. De verwerkingsverantwoordelijke is verantwoordelijk voor het bepalen van de wettelijke basis en het doel van de verwerking.
- 2. Gegevens met betrekking tot producten die rechtstreeks aan eindklanten worden aangeboden:** Bij de verwerking van persoonsgegevens in relatie tot producten die rechtstreeks aan eindklanten worden verkocht, neemt Pearson de rol van verwerkingsverantwoordelijke op zich. In dergelijke gevallen beroept zij zich op drie belangrijke rechtsgronden voor gegevensverwerking: toestemming, de uitvoering van een overeenkomst en gerechtvaardigd belang. Deze aanpak stelt Pearson in staat om te voldoen aan alle toepasselijke voorschriften inzake gegevensbescherming en om tegelijkertijd de hoogste standaarden van privacy en beveiliging voor zijn klanten te handhaven.

Voor de toepassing van de bovenstaande paragraaf gelden de volgende definities:

"Aanbieder en Testleider": een gekwalificeerde klant of een persoon die door de gekwalificeerde klant is aangewezen en gemachtigd om de testafname en scoring uit te voeren en te beheren en/of om testresultaten en rapportages te ontvangen.

"Patiënt of Kandidaat": een persoon bij wie een klinisch diagnostische test wordt afgenomen door een testleider.

Voor meer informatie over de categorieën van gegevensverwerking, het doel en de rechtsgrondslag, wordt verwezen naar de [Clinical Privacy Statement \(US\)](#).

Veilige opslagcontroles en -technologieën

Pearson en zijn sub-verwerkers zetten zich in voor de bescherming van persoonsgegevens die via Pearson Clinical platformen worden verzameld, door passende operationele, administratieve, technische en fysieke beveiligingsmaatregelen te nemen om verlies, misbruik of wijziging van de informatie in hun beheer te voorkomen. De aanpak omvat het versleutelen van alle gevoelige gegevensoverdrachten en het beveiligen van alle gegevensopslagplaatsen. Met behulp van HTTPS-versleuteling worden persoonlijke gegevens beschermd, vanaf de browser van een klant tot aan de servers van Pearson.

Wanneer betalingsgegevens worden verwerkt, beschermt Pearson deze gegevens volgens de PCI-standaarden (*Payment Card Industry*). Wanneer Pearson derden gebruikt om persoonsgegevens te verwerken, zorgt Pearson ervoor dat deze derden over passende technische en organisatorische controle beschikken om de persoonsgegevens die zij verwerken te beschermen.

Bovendien maken de servers van Pearson gebruik van Secure Sockets Layer (SSL) encryptietechnologie, die compatibel is met de meeste grote browsers en die is ontworpen om de

persoonlijke gegevens en privacy van de klant te beschermen.

Om de gegevens van klanten optimaal te beveiligen, maakt de database van de Pearson Clinical platformen gebruik van *Advanced Encryption Standard* (AES) 256-bits encryptie, een algemeen erkende en vertrouwde versleutelingsmethode. Deze robuuste beveiligingsmaatregel beschermt de gegevens van klanten effectief tegen ongeautoriseerde toegang en zorgt voor de vertrouwelijkheid en integriteit van de gegevens terwijl ze in het systeem worden opgeslagen.

De platformen van Pearson Clinical zijn gecertificeerd volgens ISO 27001 voor *Information Security Management*. Ons certificaat is op aanvraag verkrijgbaar.

Amazon AWS is gecertificeerd volgens SOC 2, wat aantoont hoe AWS belangrijke nalevingscontroles en -doelstellingen bereikt. Het SOC 2 rapport is op aanvraag beschikbaar.

Klik [hier](#) voor meer informatie over de beveiligingsmaatregelen van Pearson.

Gegevensoverdracht en naleving door de verwerker

Bij de overdracht van persoonsgegevens vanuit het Verenigd Koninkrijk (VK), de Europese Unie (EU) en de Europese Economische Ruimte (EER) baseert Pearson zich op de principes die worden erkend door de Algemene Verordening Gegevensbescherming (AVG), met name het adequaatheidsbesluit van de Europese Commissie (EC) en de Britse minister van Buitenlandse Zaken (*Secretary of State* (SoS)).

Tijdens het leveren van de diensten kan het voor bepaalde onderdelen in het proces nodig zijn om een gegevensverwerker in te schakelen. In dergelijke gevallen zorgt Pearson ervoor dat deze verwerkers adequate technische en organisatorische maatregelen treffen om de gegevens van zijn klanten te beschermen. De voorwaarden voor het inschakelen van deze verwerkers zijn ook afgestemd op de vereisten van de AVG en op onze contractuele verplichtingen jegens onze klanten.

Pearson werkt samen met Amazon Data Services Canada, Inc. en MongoDB Limited om hostingdiensten aan te bieden via Amazon Web Services (AWS). AWS speelt een cruciale rol bij het hosten van gegevens voor de digitale platformen van Pearson, terwijl we MongoDB Atlas gebruiken om betrouwbaar gegevensbeheer te garanderen, dat in overeenstemming is met wereldwijde standaarden voor operationele efficiëntie en privacy naleving. Alle verzamelde gegevens worden veilig opgeslagen op AWS-servers in Montreal, Canada.

De EC en SoS hebben Canadese commerciële organisaties **geïdentificeerd** als een sector in Canada met voldoende standaarden voor gegevensbescherming, waardoor de overdracht van gegevens vanuit het VK, de EU en de EER naar Canada mogelijk is en waarbij deze worden verwerkt in overeenstemming met de AVG, zonder dat aanvullende beveiligingen of autorisaties nodig zijn. Dit staat bekend als een adequaatheidsbesluit. Dit principe vormt de leidraad voor de relatie met AWS en wordt weergegeven in de **[AWS Klantovereenkomst](#)**, die het gebruik van AWS-services door Pearson regelt en die het **[AWS Addendum voor Gegevensverwerking](#)** via **[AWS Servicevoorwaarden](#)** omvat.

De platformen van Pearson Clinical maken geen gebruik van Amazon-diensten waarvoor gegevens moeten worden doorgegeven aan externe dienstverleners van Amazon. Als zodanig blijven alle gehoste gegevens op AWS-servers in Canada staan. De lijst met sub-verwerkers van Amazon wordt [hier](#) bijgehouden. Amazon is gecertificeerd volgens het *Data Privacy Framework*, klik [hier](#) voor meer informatie.

Daarnaast werken we samen met Twilio SendGrid, een e-mailservice, om de e-mailcommunicatie voor onze klanten met hun patiënten te stroomlijnen. De primaire rol van SendGrid is ervoor te zorgen dat uw e-mails de beoogde ontvangers bereiken. De inhoud van de e-mail wordt slechts tijdelijk opgeslagen, precies lang genoeg voor een succesvolle verzending. E-mailadressen worden gedurende een korte periode van 30 dagen bewaard om klik- en openpercentages te

analyseren, waarna ze onmiddellijk worden verwijderd. Deze aanpak minimaliseert de persoonlijke gegevens die door SendGrid worden bewaard. Belangrijk is dat deze gegevens worden overgedragen naar de Verenigde Staten voor e-mailrouting en leveringsdoeleinden. SendGrid is gecertificeerd volgens het *Data Privacy Framework*, wat is goedgekeurd door de Europese Commissie. Klik [hier](#) voor meer informatie over deze certificering.

De lijst met sub-verwerkers die door Twilio worden gebruikt is ook openbaar beschikbaar en de lijst kan [hier](#) worden bekeken.

We erkennen dat sommige van onze klanten bezorgd zijn dat de FISA-regelgeving van de Verenigde Staten van toepassing kan zijn op de internationale dochterondernemingen van Amazon. Pearson heeft dit uitvoerig onderzocht met behulp van de adequaatheidsbesluiten van de EU en de SoS en de uitgebreide [documentatie](#) van AWS met de beoordeling van het overdrachtseffect. Pearson heeft vastgesteld dat de FISA-regelgeving niet van toepassing is op Canadese bedrijven en dat de Canadese PIPEDA van toepassing is. Amazon heeft verder bevestigd dat geen enkel verzoek heeft geleid tot het openbaar maken van bedrijfs- of overheidsgegevens die zich buiten de Verenigde Staten bevinden aan de Amerikaanse overheid. Amazon publiceert halfjaarlijkse rapporten over informatieverzoeken die [hier](#) te vinden zijn.

Tijdens het hele proces van gegevensoverdracht wordt gebruik gemaakt van beveiligde verbindingen en encryptiestandaarden (AES256 en HTTPS) om gegevens in rust en gegevens in overdracht te beschermen. Gegevens in overdracht worden beschermd met AES128- en TLS-versleuteling en gegevens in rust worden beveiligd met AES256-versleuteling en *Federal Information Processing Standards* (FIPS). Bovendien bevatten de platformen van Pearson Clinical functies zoals twee-factor-authenticatie, sterke wachtwoordbeveiliging, automatisch uitloggen na perioden van inactiviteit en het niet verzamelen van gevoelige informatie zoals namen of Burgerservicenummers.

Klanten kunnen er zeker van zijn dat gegevensback-ups consistent worden onderhouden, waardoor continue toegang tot onze platforms 24 x 7 x 365 mogelijk is, tenzij ze ervoor kiezen om gegevens van de Pearson platformen te verwijderen. Klik [hier](#) voor meer informatie over de beveiligingsmaatregelen van Pearson.

Verder kan het interne ondersteuningsteam van Pearson, dat zich op verschillende wereldwijde locaties bevindt, af en toe toegang nodig hebben tot persoonsgegevens om technische ondersteuning te bieden. Pearson heeft een uitgebreide intra-groep overeenkomst voor gegevensoverdracht (*intra-group data transfer agreement* (IGA)) geïmplementeerd om ervoor te zorgen dat elk filiaal van Pearson zich houdt aan de relevante wetgeving inzake gegevens privacy bij het verwerken van persoonsgegevens.

Daarnaast is elke medewerker binnen Pearson verplicht om een grondige training te volgen met betrekking tot de verwerking van persoonsgegevens in overeenstemming met de relevante wetgeving. Ze zijn ook contractueel verplicht om de grootst mogelijke vertrouwelijkheid te handhaven, zodat persoonsgegevens altijd veilig en vertrouwelijk blijven.

Voor een beter inzicht in de architectuur van de platformen van Pearson Clinical kunt u ons diagram met de gegevensstroom bekijken dat beschikbaar is via deze links: [Q-global](#) en [Q-interactive](#).

Een up-to-date lijst van sub-verwerkers wordt [hier](#) online bijgehouden.

Rechten van de betrokkene

Wanneer een aanbieder of een testleider, handelend in de hoedanigheid van verwerkingsverantwoordelijke, persoonsgegevens deelt met Pearson en deze uploadt in het web portaal van de Pearson Clinical platformen, moeten alle aanvragen met betrekking tot privacy rechten rechtstreeks worden gericht aan de relevante aanbieder of testleider die de persoonsgegevens heeft gedeeld en die aan het verzoek zal voldoen. Er zijn functionaliteiten ingebouwd die het mogelijk maken om alle gegevens te kunnen exporteren.

Als een aanvraag omtrent gebruikersrechten betrekking heeft op de persoonsgegevens binnen de platformen van Pearson Clinical, dient de aanbieder of een testleider het verzoek door te sturen naar Pearson door een e-mail te sturen naar dataprivacy@pearson.com, en Pearson zal zijn deel van de aanvraag dienovereenkomstig inwilligen.

Voor Pearson producten die rechtstreeks aan eindklanten worden aangeboden, neemt Pearson echter de rol van verwerkingsverantwoordelijke op zich. De eindklant kan zijn rechten op het gebied van gegevensbescherming uitoefenen, waaronder het recht op toegang, recht op verwijdering of rechten op grond van de AVG en/of toepasselijke privacywetgeving, door contact op te nemen met Pearson zoals uiteengezet in ons Privacybeleid.

Naleving van gegevensverwijdering

Pearson erkent het grote belang van de persoonsgegevens van zijn klanten. Wanneer klanten gebruik maken van de diensten en platformen van Pearson Clinical, behouden ze de absolute controle over de gegevens die ze uploaden in het web portaal van de platformen van Pearson Clinical.

Als verwerkingsverantwoordelijke hebben klanten het voorrecht om hun gegevens te wissen wanneer dit nodig wordt geacht. Er zijn functionaliteiten ingebouwd waardoor klanten hun gegevens kunnen exporteren en verwijderen wanneer het hen uitkomt. In de hoedanigheid van gegevensverwerker zal Pearson ervoor zorgen dat alle aanvragen tot verwijdering van klanten op een snelle en grondige manier worden uitgevoerd. Bovendien zorgen we ervoor dat we ons houden aan de wettelijke termijnen om dergelijke verzoeken te voltooien, zoals uiteengezet in de regelgeving inzake gegevensbescherming.

Samengevat zijn de persoonlijke gegevens van klanten hun domein. Pearson respecteert dit principe en zorgt ervoor dat klanten de ultieme controle hebben over de bestemming van hun gegevens bij het gebruik van de platformen van Pearson Clinical.