PEARSON Benelux B.V. (Zweigniederlassung Deutschland)

und

.....

Auftragsverarbeitungsvertrag

DATUM: ..... ("Datum des Inkrafttretens")

PARTEIEN:

Dieser Auftragsverarbeitungsvertrag ("AVV") ergänzt die zwischen dem Kunden und Pearson abgeschlossenen Nutzungsbedingungen und ist Teil des Dienstvertrages ("Hauptvertrag") zwischen

(1) ..... ("Kunde")

(2) Pearson Benelux B.V. (Zweigniederlassung Deutschland) (Handelsregisternummer HRB 289576) mit Sitz in der Kaiserstraße 44, 60329 Frankfurt am Main, Deutschland ("Pearson").

(zusammen als die "Parteien" bezeichnet)

UNTER DEN FOLGENDEN ANNAHMEN:

A. Vor dem/am Datum des Inkrafttretens hat der Kunde einen oder mehrere Hauptverträge abgeschlossen, um Zugang zu bestimmten Diensten von Pearson ("Dienste") zu erwerben.

B. Ab dem Datum des Inkrafttretens ersetzt dieser AVV alle Datenschutz- oder Verarbeitungsklauseln in jedem Hauptvertrag oder früheren Auftragsverarbeitungsvertrag und wird in jeden Hauptvertrag aufgenommen.

C. Der Kunde handelt als Verantwortlicher.

D. Pearson handelt als Auftragsverarbeiter.

E. Der Kunde möchte bestimmte, im Hauptvertrag definierte Dienste, die die Verarbeitung personenbezogener Daten beinhalten, an Pearson untervergeben.

F. Die Parteien streben den Abschluss eines Auftragsverarbeitungsvertrages an, der den Anforderungen des derzeitigen Rechtsrahmens in Bezug auf die Datenverarbeitung und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) entspricht.

G. Die Parteien möchten ihre Rechte und Pflichten festlegen.

WIRD WIE FOLGT VEREINBART:

1. Definitionen und Auslegung

1.1. Sofern in diesem AVV nicht anders definiert, haben die in diesem Vertrag verwendeten Begriffe und Ausdrücke die folgende Bedeutung:

1.1.1. "**Personenbezogene Daten des Kunden**" sind personenbezogene Daten, die von Pearson als Auftragsverarbeiter oder Unterauftragsverarbeiter für und im Namen des Kunden während der Erbringung von Diensten verarbeitet werden;

1.1.2. "**Datenschutzgesetze**" bedeutet EU-Datenschutzgesetze und, soweit anwendbar, die Datenschutzgesetze anderer Länder. Diese Definition umfasst auch alle Änderungen, Aktualisierungen oder Ersetzungen

solcher Gesetze und Vorschriften sowie alle verbindlichen Entscheidungen oder Auslegungen der zuständigen Behörden, Gerichte oder Datenschutzaufsichtsbehörden;

1.1.3. **"DSGVO**" bezeichnet die EU-Datenschutzgrundverordnung 2016/679;

1.1.4. **"Datenübermittlung**" bedeutet:

1.1.4.1. eine Übermittlung Personenbezogener Daten des Kunden vom Kunden an Pearson; oder

1.1.4.2. eine Weitergabe Personenbezogener Daten des Kunden von Pearson an einen Unterauftragsverarbeiter oder zwischen zwei Niederlassungen von Pearson;

1.1.5. **"Sicherheitsvorfall**" bedeutet eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung oder zur unbefugten Offenlegung von oder zum Zugriff auf Personenbezogene Daten des Kunden führt. Sicherheitsvorfälle umfassen keine erfolglosen Versuche oder Aktivitäten, die die Sicherheit von verschlüsselten Personenbezogenen Daten des Kunden nicht beeinträchtigen;

1.1.6. "**Standardvertragsklauseln"** oder **"(SCCs)"** bezeichnet die Vertragsklauseln im Anhang des Durchführungsbeschlusses 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, die derzeit unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj zu finden sind.

1.1.7. **"Unterauftragsverarbeiter**" bezeichnet jede Stelle, die vom Auftragsverarbeiter oder in dessen Namen beauftragt wird, personenbezogene Daten im Namen des Kunden in Verbindung mit dem Vertrag zu verarbeiten.

1.1.8. Die Begriffe "**Kommission**", "**für die Verarbeitung Verantwortlicher**", "**betroffene Person**", "**Mitgliedstaat**", "**personenbezogene Daten**", "**Verletzung des Schutzes personenbezogener Daten**", "**Auftragsverarbeiter**", "**Verarbeitung**" und "**Aufsichtsbehörde**" haben dieselbe Bedeutung wie in der DSGVO, und ihre verwandten Begriffe sind entsprechend auszulegen.

2. Weisungen für die Verarbeitung

2.1. In Anbetracht der Tatsache, dass der Kunde Pearson die Personenbezogenen Daten des Kunden zur Verfügung stellt, erklärt sich Pearson bereit, die Personenbezogenen Daten des Kunden in Übereinstimmung mit den Bedingungen dieses AVV und wie in Anhang 1 dargelegt zu verarbeiten, um den Hauptvertrag zu erfüllen.

2.2. Vorbehaltlich der Klausel 2.3 erkennen die Parteien an und vereinbaren, dass:

2.2.1. für die Zwecke dieses AVV und im Verhältnis zwischen ihnen der Kunde als Verantwortlicher für die Personenbezogenen Daten des Kunden, und Pearson als Auftragsverarbeiter oder Unterauftragsverarbeiter der Personenbezogenen Daten des Kunden zu sehen ist;

2.2.2. Der Kunde wird alle geltenden Datenschutzgesetze und seine Verpflichtungen als der für die Verarbeitung Verantwortlicher einhalten;

2.2.3. Pearson wird bei der Verarbeitung Personenbezogener Daten des Kunden alle geltenden Datenschutzgesetze einhalten; und

2.2.4. Pearson verarbeitet die Personenbezogenen Daten des Kunden nur auf der Grundlage der entsprechenden dokumentierten Anweisungen des Kunden, es sei denn, dies ist durch geltende Gesetze vorgeschrieben.

2.3. Wenn der Kunde ein Auftragsverarbeiter ist, garantiert er Pearson, dass die Anweisungen und Handlungen des Kunden in Bezug auf die Personenbezogenen Daten des Kunden, einschließlich der Ernennung von Pearson als weiteren Auftragsverarbeiter, von dem entsprechenden Verantwortlichen genehmigt wurden und mit den geltenden Datenschutzgesetzen in Einklang stehen.

2.4. Der Kunde weist Pearson an und Pearson erklärt sich bereit, die Personenbezogenen Daten des Kunden zu verarbeiten, um die im Hauptvertrag genannten Dienste zu erbringen.

3. Mitarbeiter von Pearson

3.1. Pearson ergreift angemessene Maßnahmen, um die Zuverlässigkeit aller Mitarbeiter, Vertreter oder Auftragnehmer von Pearson zu gewährleisten, die Zugang zu den Personenbezogenen Daten des Kunden haben, und stellt in jedem Fall sicher, dass der Zugang strikt auf die Personen beschränkt ist, die die betreffenden Personenbezogenen Daten des Kunden kennen/auf sie zugreifen müssen, soweit dies für die Zwecke des Hauptvertrags unbedingt erforderlich ist, und um die geltenden Gesetze im Zusammenhang mit den Pflichten dieser Personen gegenüber Pearson einzuhalten.

3.2. Pearson stellt sicher, dass alle Personen, die Pearson zur Verarbeitung Personenbezogener Daten des Kunden ermächtigt, einer Vertraulichkeitsverpflichtung oder einer beruflichen oder gesetzlichen Verschwiegenheitspflicht unterliegen und Personenbezogene Daten des Kunden nur gemäß den Bestimmungen dieses AVVs verarbeiten.

4. Rechte der betroffenen Person

4.1. Unter Berücksichtigung der Art der Verarbeitung unterstützt Pearson den Kunden, indem Pearson, soweit dies möglich ist, geeignete technische und organisatorische Maßnahmen ergreift, um die Verpflichtungen des Kunden, so wie er sie vernünftigerweise verstanden hat, zu erfüllen, um auf Anfragen zur Ausübung von Rechten der betroffenen Person gemäß den Datenschutzgesetzen zu reagieren.

4.2. Pearson:

4.2.1. benachrichtigt den Kunden unverzüglich, wenn er eine Anfrage von einer betroffenen Person gemäß einem Datenschutzgesetz in Bezug auf die Personenbezogenen Daten des Kunden erhält, und der Kunde für die Beantwortung einer solchen Anfrage verantwortlich ist; und

4.2.2. stellt sicher, dass Pearson diese Anfrage nur auf dokumentierte Anweisungen des Kunden oder gemäß den geltenden Gesetzen, denen Pearson unterliegt, beantwortet; in diesem Fall informiert Pearson den Kunden, soweit dies nach den geltenden Gesetzen zulässig ist, über diese gesetzlichen Anforderungen, bevor Pearson auf die Anfrage antwortet.

4.3. Pearson gibt keine personenbezogenen Daten des Kunden auf Anfrage eines Dritten ohne dessen vorherige schriftliche Zustimmung weiter, es sei denn, der Kunde ist nach geltendem Recht dazu gezwungen oder ist anderweitig im Rahmen dieser DPA oder der Vereinbarung dazu berechtigt.

5. Sicherheitsmaßnahmen

5.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos variierender Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen ergreift Pearson in Bezug auf die Personenbezogenen Daten des Kunden geeignete technische und organisatorische Maßnahmen, um ein diesem Risiko angemessenes Sicherheitsniveau zu gewährleisten, einschließlich sofern geeignet, der in Artikel 32 Absatz 1 DSGVO genannten Maßnahmen.

5.2. Bei der Bewertung des angemessenen Sicherheitsniveaus berücksichtigt Pearson insbesondere die Risiken, die sich aus der Verarbeitung ergeben, insbesondere aus einer Verletzung des Schutzes personenbezogener Daten.

5.3. Die technischen, sicherheitstechnischen und organisatorischen Maßnahmen, auf die in Abschnitt 5.1 Bezug genommen wird, müssen mindestens die in Anhang 3 aufgeführten Sicherheitsanforderungen erfüllen.

5.4. Die Grundsätze und Empfehlungen der ISO-Norm 27001 (mit späteren Änderungen) sollten als Rahmenrichtlinie für die Erfüllung der Anforderungen dieses AVVs dienen.

6. Sicherheitsvorfälle

6.1. Pearson benachrichtigt den Kunden über jeden Sicherheitsvorfall, von dem Person Kenntnis erlangt, unverzüglich und spätestens 48 Stunden nach Bekanntwerden des Sicherheitsvorfalls. Alle derartigen Benachrichtigungen sollten in Übereinstimmung mit den in diesem AVV festgelegten Benachrichtigungsbestimmungen oder nach Ermessen von Pearson durch einen Anruf oder eine E-Mail an den Vertreter des Kunden erfolgen, mit dem Pearson regelmäßig in Kontakt steht.

6.2. Pearson ergreift angemessene Maßnahmen, um die Auswirkungen von Sicherheitsvorfällen zu beheben oder zu mindern.

6.3. Pearson kooperiert mit dem Kunden und stellt ihm angemessene Unterstützung und Informationen zur Verfügung:

6.3.1. bei der Untersuchung eines Sicherheitsvorfalls; und

6.3.2. in Bezug auf alle Meldungen eines Sicherheitsvorfalls, die der Kunde an eine Aufsichtsbehörde macht.

6.4. Alle Kosten, die mit der Bewältigung eines Sicherheitsvorfalls und der Erfüllung der daraus entstehenden Verpflichtungen verbunden sind, sind vom Kunden zu tragen, wenn der Sicherheitsvorfall darauf zurückzuführen ist, dass der Kunde seine Verpflichtungen im Rahmen dieses AVVs nicht erfüllt hat oder dass die autorisierten Nutzer des Kunden die Nutzungsbedingungen der Dienste nicht eingehalten haben.

6.5. Der Kunde ist allein dafür verantwortlich, dass er alle Gesetze zur Meldung von Vorfällen in Bezug auf die Personenbezogenen Daten des Kunden einhält und alle Meldepflichten gegenüber Dritten im Zusammenhang mit Sicherheitsvorfällen erfüllt.

6.6. Die Benachrichtigung von Pearson über einen Sicherheitsvorfall oder die Reaktion auf einen Sicherheitsvorfall gemäß dieser Klausel ist nicht als Anerkenntnis eines Fehlers oder einer Haftung von Pearson in Bezug auf diesen Sicherheitsvorfall auszulegen.

7. Unterauftragsverarbeiter

7.1. Pearson darf anderen Unternehmen der Pearson-Gruppe, Unterauftragsverarbeitern oder sonstigen Dritten keinen Zugang zur Verarbeitung personenbezogener Kundendaten gewähren, diese offenlegen oder sie damit beauftragen, es sei denn:

7.1.1. der Kunde erteilt ausdrücklich eine vorherige schriftliche Genehmigung;

7.1.2. Pearson erlegt dem Unternehmen der Pearson-Gruppe, dem Unterauftragsverarbeiter oder anderen Dritten Bedingungen auf, die nicht weniger verpflichtend sind als die, die Pearson im Rahmen dieser Vereinbarung auferlegt werden;

7.2. Ungeachtet der Klausel 7.1 gilt ab dem Datum dieser Vereinbarung:

7.2.1. Der Kunde stimmt den in Anhang 2 aufgeführten Konzerngesellschaften von Pearson zu;

7.2.2. Der Kunde stimmt den in dem beigefügten Anhang 2 aufgeführten Unterauftragsverarbeitern zu; und

7.2.3. Pearson sichert zu, dass Pearson den Unternehmen der Pearson-Gruppe und den aufgeführten Unterauftragsverarbeitern Datenschutzbestimmungen gemäß 7.1 auferlegt hat.

7.3. Pearson muss den Kunden benachrichtigen und dessen ausdrückliche schriftliche Zustimmung einholen, wenn Pearson einen neuen Unterauftragsverarbeiter einsetzen möchte, der derzeit nicht in Anhang 2 oder auf der Website von Pearson aufgeführt ist. Die Mitteilung muss mindestens 60 Tage, bevor Pearson den neuen Unterauftragsverarbeiter einsetzen will, eingehen.

7.4. Pearson haftet in vollem Umfang für Verstöße gegen diesen AVV, die durch eine Handlung, einen Fehler oder eine Unterlassung eines seiner Unterauftragsverarbeiter bei der Verarbeitung Personenbezogener Daten des Kunden verursacht werden.

8. Datenschutz-Folgenabschätzungen und vorherige Konsultation

8.1. Pearson unterstützt den Kunden in angemessener Weise bei allen Risikobewertungen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen mit Aufsichtsbehörden oder anderen zuständigen Datenschutzbehörden, die der Kunde nach vernünftigem Ermessen gemäß Artikel 32, 35 oder 36 DSGVO oder gleichwertigen Bestimmungen anderer Datenschutzgesetze für erforderlich hält, und zwar jeweils ausschließlich in Bezug auf die Verarbeitung Personenbezogener Daten des Kunden durch Pearson und unter Berücksichtigung der Art der Verarbeitung und der Pearson vorliegenden Informationen.

9. Prüfrechte

9.1. Auf Verlangen des Kunden und höchstens einmal jährlich stellt Pearson dem Kunden alle angemessenen Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesem AVV festgelegten Verpflichtungen nachzuweisen, und ermöglicht Prüfungen, einschließlich Inspektionen, die vom Kunden oder einem anderen vom Kunden beauftragten Prüfer durchgeführt werden, und trägt zu diesen Prüfungen bei.

9.2. Auf Verlangen des Kunden stellt Pearson dem Kunden kostenlos die Dokumentation der Dienste zur Verfügung, in der die Sicherheits- und Datenschutzpraktiken von Pearson sowie die einschlägigen Zertifizierungen wie ISO 27001 und SOC-II-Bericht beschrieben sind. Der Kunde erkennt an, dass mit der Bereitstellung dieser Dokumente die in Artikel 28 Absatz 3 lit. h) DSGVO festgelegten Prüfungsanforderungen oder andere in einem Vertrag zwischen den Parteien enthaltene Verpflichtungen in Bezug auf Datenschutz oder Informationssicherheit erfüllt sind.

9.3. Verlangt der Kunde eine weitere Überprüfung, einschließlich eines Audits oder einer Inspektion der Datenverarbeitungseinrichtungen von Pearson, so vereinbaren Pearson und der Kunde den Zeitpunkt, den Umfang und die Sicherheits- und Vertraulichkeitskontrollen, die für eine solche Überprüfung oder Inspektion gelten.

9.4. Pearson kann für eine solche Überprüfung oder Inspektion eine Gebühr gemäß Klausel 9.3 erheben und wird den Kunden vor einer solchen Überprüfung oder Inspektion über die anfallenden Gebühren informieren. Der Kunde trägt für alle mit einer solchen Überprüfung oder Inspektion verbundenen Kosten.

10. Internationale Datenübermittlung

10.1. Im Zuge der Erbringung der Dienste erkennt der Kunde an, dass Pearson und/oder seine Unterauftragsverarbeiter Verarbeitungstätigkeiten außerhalb des Herkunftslandes der

Personenbezogenen Daten des Kunden durchführen können und dass Personenbezogene Daten des Kunden in Ländern erhoben, verarbeitet und/oder gespeichert werden können, in denen die geltenden Gesetze in Bezug auf die Verarbeitung personenbezogener Daten von denen des Herkunftslandes abweichen können. Pearson stellt sicher, dass solche Übermittlungen in Übereinstimmung mit genehmigten rechtlichen Mechanismen und in Übereinstimmung mit den Anforderungen der geltenden Datenschutzgesetze und DSGVO, einschließlich aller späteren Gesetzesänderungen oder -erlasse, erfolgen.

10.2. Wenn und soweit die DSGVO auf die Verarbeitung der Personenbezogenen Daten des Kunden, die Gegenstand einer internationalen Datenübermittlung sind, Anwendung findet, wird Pearson die Personenbezogenen Daten des Kunden nur an Empfänger übermitteln, die über angemessene Sicherheitsvorkehrungen verfügen, wozu auch gehören können:

10.2.1. Eine Angemessenheitsentscheidung der Europäischen Kommission

10.2.2. Von der Europäischen Kommission genehmigte Standardvertragsklauseln

10.2.3. Verbindliche interne Datenschutzvorschriften

11. Beginn und Dauer der Vereinbarung

11.1. Dieser AVV tritt in Kraft, sobald er von beiden Parteien unterzeichnet wurde.

11.2. Dieser AVV ist so lange in Kraft, wie die Verarbeitung personenbezogener Daten durchgeführt wird, und dieser AVV muss bis zur Beendigung der Verarbeitung in Kraft bleiben.

11.3. Der Kunde weist Pearson an, die Personenbezogenen Daten des Kunden für einen angemessenen Zeitraum nach der Beendigung oder dem Auslaufen des Hauptvertrags aufzubewahren, um eine spätere Prüfung oder Datenwiederherstellung zu unterstützen, die der Kunde möglicherweise benötigt.

11.4. Danach vernichtet Pearson die Personenbezogenen Daten des Kunden, die sich in seinem Besitz oder unter seiner Kontrolle befinden, oder gibt sie zurück. Die Verpflichtung (zur Vernichtung von Daten) gilt nicht, soweit Pearson aufgrund seiner internen Richtlinien oder aufgrund von Gesetzen der Europäischen Union (oder eines Mitgliedstaates der Europäischen Union) oder anderen anwendbaren Gesetzen oder aufgrund von vertraglichen Verpflichtungen nach Beendigung der Vereinbarung verpflichtet ist, einige oder alle Personenbezogenen Daten des Kunden aufzubewahren. Die Bestimmungen dieses AVVs gelten weiterhin für alle Personenbezogenen Daten des Kunden, die von Pearson aufbewahrt werden, ungeachtet der Beendigung oder des Ablaufs des Hauptvertrags.

11.5. Wenn Pearson oder ein Unterauftragsverarbeiter Insolvenz, Liquidation oder Ähnliches erleidet und daher die Verarbeitung personenbezogener Daten für den Kunden einstellt, müssen alle personenbezogenen Daten unverzüglich an den Kunden in einer Weise zurückgegeben werden, die es dem Kunden ermöglicht, sie weiterhin zu nutzen. Der Kunde hat auch die Möglichkeit, alle personenbezogenen Daten direkt über das System zu exportieren und zu speichern. Im Anschluss daran ist Pearson, der überschuldete Nachlass o.ä., verpflichtet, die personenbezogenen Daten in Übereinstimmung mit dem Vorstehenden aus seinen Systemen zu löschen.

12. Verwendung von de-identifizierten Daten

12.1. Der Kunde erklärt sich damit einverstanden, dass Pearson während und nach Ablauf des Hauptvertrags Personenbezogene Daten des Kunden, aus denen Merkmale zur direkten Identifizierung einer Person entfernt wurden und die somit als anonymisierte Daten gelten, für Benchmarking, Bildungsforschung, Entwicklung und Verbesserung von Produkten und Diensten oder für andere damit verbundene Zwecke verwenden und offenlegen darf. Solche anonymisierten Daten gelten nicht als Personenbezogene Daten des Kunden.

13. **Vertraulichkeit**

13.1. Jede Partei muss diesen AVV und die Informationen, die sie im Zusammenhang mit diesem AVV über die andere Partei und deren Geschäfte erhält ("Vertrauliche Informationen"), vertraulich behandeln und darf diese Vertraulichen Informationen nicht ohne die vorherige schriftliche Zustimmung der anderen Partei verwenden oder offenlegen, es sei denn:

13.1.1. die Offenlegung ist gesetzlich vorgeschrieben;

13.1.2. die entsprechenden Informationen sind bereits öffentlich zugänglich.

14. **Benachrichtigungen und Mitteilungen**

14.1. Alle Benachrichtigungen und Mitteilungen im Rahmen dieses AVVs erfolgen schriftlich durch persönliche Übergabe, Eilkurier, bestätigte E-Mail oder Einschreiben mit Rückschein und gelten bei persönlicher Übergabe, einen (1) Tag nach Abgabe bei einem Eilkurier, nach Bestätigung des Empfangs der E-Mail oder fünf (5) Tage nach Hinterlegung auf dem Postweg als erfolgt. Die Benachrichtigungen und Mitteilungen werden an die eingetragene Anschrift der Vertragspartei oder an eine andere von ihr schriftlich angegebene Anschrift gesandt.

15. Auswirkung der Ergänzungen

15.1. Mit Wirkung vom Datum des Inkrafttretens ersetzt diese AVV-Änderung alle Datenschutzbestimmungen in jeder Hauptvereinbarung und/oder früheren Datenverarbeitungsvereinbarung und wird in jeden Hauptvertrag aufgenommen. Im Falle von Konflikten oder Widersprüchen zwischen den Bestimmungen dieses AVVs und den übrigen Bestimmungen des jeweiligen Hauptvertrages sind die Bestimmungen dieses AVVs maßgeblich. Vorbehaltlich der Änderungen in diesem AVV bleibt jeder Hauptvertrag in vollem Umfang in Kraft und wirksam. Wenn der Kunde mehr als einen Hauptvertrag abgeschlossen hat, wird dieser AVV jeden Hauptvertrag separat ändern.

UNTERSCHRIFT für und im Namen des Kunden

Unterschrift

Name in Druckschrift

Titel

UNTERSCHRIFT für und im Namen von Pearson Benelux B.V. (Zweigniederlassung Deutschland)

Unterschrift

Name in Druckschrift

Titel

Anhang 1 – Weisungen für den Auftragsverarbeiter

1. Weisungen

1.1. Der Kunde weist Pearson hiermit an, die Personenbezogenen Daten des Kunden für den Betrieb der Dienste wie im Hauptvertrag beschrieben zu verarbeiten.

1.2. Wenn Pearson die Verarbeitung Personenbezogenen Daten des Kunden an Unterauftragsverarbeiter überträgt, die gemäß Anhang 2 zugelassen sind, ist Pearson dafür verantwortlich, schriftliche Vereinbarungen mit diesen zu treffen, die Bedingungen in Einklang mit diesem AVV enthalten.

2. Zweck der Verarbeitung

2.1.1. Die Verarbeitung der Personenbezogenen Daten des Kunden erfolgt zu folgenden spezifischen Zwecken: Zur Erleichterung der Bereitstellung des klinischen Bewertungssystems, das es dem Kunden ermöglicht, klinische Bewertungen wie im Hauptvertrag beschrieben durchzuführen.

2.1.2. Bereitstellung von Kundensupport und technischer Unterstützung im Zusammenhang mit der Nutzung des klinischen Bewertungssystems.

2.2. Pearson verarbeitet die Personenbezogenen Daten des Kunden in Übereinstimmung mit den genannten Zwecken und allen weiteren vom Kunden erteilten Anweisungen.

2.3. Pearson darf die Personenbezogenen Daten des Kunden nicht für andere Zwecke verwenden.

2.4. Die Personenbezogenen Daten des Kunden dürfen nicht nach anderen Anweisungen als denen des Kunden verarbeitet werden.

3. Allgemeine Beschreibung der Verarbeitung

Q-interaktive

3.1. Die Tests finden auf zwei iPads in einer App namens Assess statt. Der Administrator verwendet das eine iPad, um auf die Anweisungen der Testverwaltung zuzugreifen, die Antworten zu bewerten und aufzuzeichnen und die visuellen Stimuli zu steuern. Der Prüfling verwendet das andere iPad, um die Stimuli zu sehen und darauf zu reagieren.

3.2. Q-interactive umfasst auch eine Website, über die Berichte für die auf den iPads durchgeführten Bewertungen erstellt und Daten langfristig gespeichert werden können.

3.3. Der Administrator kann neue Benutzer anlegen, ihnen Lizenzen zuweisen, die Nutzung des Kontos verfolgen und die Testdaten aller Prüflinge des Kontos einsehen.

3.4. Q-interactive verfügt auch über eine Administrator-Assistenten-Rolle. Administrator-Assistenten können Benutzer anlegen, ihnen Lizenzen zuweisen und die Nutzung verfolgen, aber sie können keine Prüfungsdaten der Prüflinge sehen.

Q-global

3.5. Eine Website bietet die Möglichkeit, neue Prüflinge anzulegen und die Daten eines durchgeführten Tests manuell zu registrieren, um einen digitalen Bericht zu erhalten, der lokal gespeichert und/oder ausgedruckt werden kann.

4. Kategorien von personenbezogenen Daten

Die Verarbeitung umfasst personenbezogene Daten der unten angekreuzten Kategorien.

Personenbezogene Daten

☒ Name

☒ Geburtsdatum

☒ E-Mail-Adresse

☒ Telefon-Nummer

☐ Postanschrift

☐ Nationale Identifikationsnummer

☐ Ausweisdokumente (z. B. Reisepass oder Führerschein)

☐ Finanz-Informationen

☐ Informationen zu Konten in sozialen Medien

☐ Beschäftigungshistorie und berufsbezogene Informationen

☐ Ausbildung und akademische Leistungen

Besondere Kategorien personenbezogener Daten

☒ Rasse oder ethnische Herkunft

☐ Politische Meinungen

☐ Religiöse Überzeugungen

☐ Philosophische Überzeugungen

☐ Mitgliedschaft in einer Gewerkschaft

☒ Gesundheitsbezogene Daten

☐ Daten zum Sexualleben oder zur sexuellen Orientierung

5. Kategorien betroffener Personen

5.1. Es werden Daten über die folgenden Kategorien betroffener Personen verarbeitet:

5.1.1. Ein Anbieter/Administrator von Prüfungen, z. B. Psychologen und anders Fachpersonal aus dem Gesundheitswesen.

5.1.2. Ein Patient/Prüfling, der sich einer Untersuchung durch Psychologen und anderes Fachpersonal aus dem Gesundheitswesen unterzieht, die Q-interactive verwenden.

6. Drittländer (Nicht-EU-Mitgliedstaaten)

6.1. Pearson kann personenbezogene Daten in die folgenden Drittländer übermitteln:

6.1.1. Kanada

6.2. Ein angemessenes Schutzniveau wird durch den Angemessenheitsbeschluss der EU-Kommission von 2001 in Bezug auf kanadische Privatunternehmen gewährleistet.

Anhang 2 - Pearsons Unterauftragsverarbeiter

Pearson setzt den/die folgenden Unterauftragsverarbeiter in Verbindung mit den Aufgaben ein, die Pearson für den Kunden ausführt. Mit dem Abschluss des AVVs stimmt der Kunde der Nutzung dieser Unterauftragsverarbeiter zu.

Eine Tabelle pro Sub-Prozessor.

	Name des Unternehmens	Reg.-Nr.	Adresse	Beschreibung der Verarbeitung	Transfer-Mechanismus
Unterauftrags-verarbeiter (1. Stufe)	Amazon Web Services Canada, Inc.	857305932	120 Bremner Blvd, 26. Stock, Toronto, ON, M5J 0A8, Kanada	Cloud Computing-Dienste und Betrieb von Rechenzentren. Hosting von Personenbezogenen Daten des Kunden. Vom Kunden initiierte Unterstützung. Zugriff auf Daten nur mit ausdrücklicher Zustimmung des Kunden zum Zeitpunkt der Anfrage.	Angemessenheitsentscheidung der Europäischen Union
Unterauftrags-verarbeiter (2. Stufe)	Amazon Data Services Canada, Inc.	797963121	160 Elgin Street Suite 2600, Ottawa, ON, K1P 1C3	Cloud Computing-Dienste und Betrieb von Rechenzentren. Hosting von Personenbezogenen Daten des Kunden.	Angemessenheitsentscheidung der Europäischen Union

	Name des Unternehmens	Reg.-Nr.	Adresse	Beschreibung der Verarbeitung	Transfer-Mechanismus
Unterauftrags-verarbeiter (1. Stufe)	Bahnhof	831671	Sveavagen 41, 111 40 Stockholm, Schweden	Hosting von Personenbezogenen Daten des Kunden.	K.A.
Unterauftrags-verarbeiter (2. Stufe)	Keine				

	Name des Unternehmens	Reg.-Nr.	Adresse	Beschreibung der Verarbeitung	Transfer-Mechanismus
Unterauftrags-verarbeiter (1. Stufe)	SendGrid von Twilio (Twilio Ireland Limited)	IE557454	3 Dublin Landings, North Wall Quay, Dublin 1, Irland	Weiterleitung und Übermittlung von E-Mails. In E-Mails enthaltene personenbezogene Daten werden an die Ziel-E-Mail übermittelt. Die Daten des E-Mail-Textes werden nur so lange aufbewahrt, wie es für den Versand der E-Mail erforderlich ist. Die Ziel-E-Mail-Adresse wird zu Analysezwecken aufbewahrt.	Angemessenheitsentscheidung der Europäischen Union – Data Privacy Framework
Unterauftrags-verarbeiter (2. Stufe)	AWS Amazon USA	0000174230	410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.	Hosting von SendGrid-Daten.	Angemessenheitsentscheidung der Europäischen Union – Data Privacy Framework

	Name des Unternehmens	Reg.-Nr.	Adresse	Beschreibung der Verarbeitung	Transfer-Mechanismus
Unterauftrags-verarbeiter (1. Stufe)	MongoDB-Atlas (MongoDB Limited)	4999921	Gebäude zwei, Nummer eins, Ballsbridge, Shellbourne Road, Dublin 4, Co Dublin, Irland	Datenbank als Dienstleistung für das Hosting von Personenbezogenen des Kunden.	K.A.
Unterauftrags-verarbeiter (2. Stufe)	Amazon Web Services Canada, Inc.	857305932	120 Bremner Blvd, 26. Stock, Toronto, ON, M5J	Hosting von MongoDB Atlas Daten.	Angemessenheitsentscheidung der Europäischen Union

			0A8, Kanada		

	Name des Unternehmens	Reg.-Nr.	Adresse	Beschreibung der Verarbeitung	Transfer-Mechanismus
Unterauftrags-verarbeiter (Unternehmen der Pearson-Gruppe)	Pearson Education Limited (UK)	872828	80 Strand, London, WC2R 0RL, Vereinigtes Königreich	Kundensupport. Zugang zu Prüfungs-/Bewertungsdaten nur mit ausdrücklicher Zustimmung des Kunden zum Zeitpunkt der Anfrage.	Angemessenheitsentscheidung der Europäischen Union Alle Pearson-Einheiten sind durch unser unternehmensübergreifendes International Data Transfer Agreement (IDTA) gebunden.
Unterauftrags-verarbeiter (Unternehmen der Pearson-Gruppe)	Pearson Canada Assessment Inc. (Canada)	1163650766	176 Yonge Street, 6. Stock, Toronto, ON, M5C 2L7, Kanada	Technischer Support.	Angemessenheitsentscheidung der Europäischen Union Alle Pearson-Einheiten sind durch unser unternehmensübergreifendes International Data Transfer Agreement (IDTA) gebunden.
Unterauftrags-verarbeiter (Unternehmen der Pearson-Gruppe)	NCS Pearson, Inc. (USA)	410850527	5601 Green Valley Drive, Bloomington, MN 55437, U.S.A.	Technischer Support aus der dritten Ordnung. Zugang zu den Daten der Prüflinge/Bewertungen nur mit ausdrücklicher Zustimmung des Kunden zum Zeitpunkt der Anfrage.	Alle Pearson-Einheiten sind durch unser unternehmensübergreifendes International Data Transfer Agreement (IDTA) gebunden.

Anhang 3 - Anforderungen an die Informationssicherheit

1. Allgemeine Sicherheitsanforderungen. Pearson:

1.1. Hält die geltenden gesetzlichen Bestimmungen und die von der Branche vorgeschriebenen Informationssicherheitsstandards (Beispiele für solche Standards sind u. a. ISO/IEC 27001, die Payment Card Industry-Data Security Standards (PCI-DSS), EDI-Standards (Electronic Data Interchange) und die in Gesetzen wie dem Health Insurance Portability and Accountability Act (HIPAA) dokumentierten Informationssicherheitsanforderungen) ein.

1.2. Führt Ein formelles und umfassendes Sicherheitsprogramm in Übereinstimmung mit den Best Practices der Branche mit angemessenen und geeigneten administrativen, organisatorischen, technischen und physischen Sicherheitsvorkehrungen ein und hält es aufrecht, einschließlich der in diesem Anhang 3 dargelegten Vorkehrungen ("Anforderungen an die Informationssicherheit"), um die Vertraulichkeit, Integrität und Verfügbarkeit der Personenbezogenen Daten des Kunden (einschließlich, aber nicht beschränkt auf den Schutz der Personenbezogenen Daten des Kunden) zu gewährleisten und Sicherheitsvorfälle zu verhindern. Diese Datensicherheitsmaßnahmen umfassen unter anderem Folgendes:

1.2.1. Pearson führt ein Verzeichnis der Systeme, die von Pearson zur Speicherung oder Verarbeitung Personenbezogener Daten des Kunden verwendet werden;

1.2.2. Alle Ausdrucke, die Personenbezogene Daten des Kunden oder damit zusammenhängenden Support der Anwendung enthalten, sind bei Nichtgebrauch in verschlossenen Behältnissen/Containern zu sichern und jederzeit während oder am Ende der Laufzeit dieses AVVs oder auf Wunsch des Kunden durch sichere Vernichtung zu vernichten. Der Kunde kann eine Bescheinigung über die Vernichtung verlangen;

1.2.3. Kundendaten von den Daten und Informationen anderer Kunden oder von Pearson selbst trennen;

1.2.4. über dokumentierte Verfahren für die sichere Speicherung und Wiederherstellung Personenbezogener Daten des Kunden verfügen, die mindestens eine starke Verschlüsselung sowie sichere Verfahren für den Transport, die Lagerung und die Entsorgung der Sicherungskopien personenbezogener Daten des Kunden mit dokumentierter Aufbewahrungskette umfassen müssen.

1.2.5. Verwendet eine starke Verschlüsselung, um personenbezogene Daten bei der Übermittlung und Speicherung zu schützen.

2. Sicherheit des Personals oder der Mitarbeiter

2.1. Pearson führt, soweit gesetzlich zulässig, eine umfassende Hintergrundprüfung aller Mitarbeiter durch, bevor sie Zugang zu Personenbezogenen Daten des Kunden erhalten, einschließlich der Überprüfung der Identität, der Adresse, des Beschäftigungsverlaufs/der Eignung und der beruflichen Qualifikationen aller Mitglieder des Pearson-Teams sowie der Durchführung zusätzlicher Überprüfungen wie Drogenscreenings oder Strafregisterauszüge (soweit verfügbar);

2.2. Pearson verfügt über eine förmliche Richtlinie zu den Bedingungen und Fristen für den Zugang zu Kunden- oder Pearson-Systemen, der Personen, die neu hinzukommen gegeben wird, der für Personen, die eine andere Rolle übernehmen, geändert wird und der für Personen, die aus irgendeinem Grund ausscheiden, aufgehoben wird.

2.3. Pearson stellt sicher, dass alle autorisierten Personen über eine relevante, angemessene und notwendige Ausbildung und Erfahrung verfügen.

2.4. Pearson stellt sicher, dass alle bevollmächtigten Personen, die mit Personenbezogenen Daten des Kunden umgehen, über die Vertraulichkeit der Personenbezogenen Daten des Kunden informiert sind und eine angemessene Schulung in Bezug auf ihre Pflichten im Zusammenhang mit dem Umgang mit diesen Daten absolviert haben, einschließlich geltender Gesetze und Vorschriften, potenzieller Sicherheits- oder Meldepflichten bei Datenschutzverletzungen sowie akzeptabler Nutzung und angemessener Verfahren für die Speicherung und Übermittlung Personenbezogener Daten des Kunden. Pearson führt Aufzeichnungen über diese Schulung und stellt diese Aufzeichnungen dem Kunden auf Anfrage zur Verfügung.

3. Sicherheit der Systeme. Pearson:

3.1. hält sich, sofern geeignet, an das gemeinsame Sicherheitsmodell seines Cloud-Hosting-Anbieters und an die von der Cloud Security Alliance, Cloud Control Matrix, beschriebenen bewährten Praktiken.

3.2. schützt Personenbezogene Daten des Kunden durch die Implementierung von Informationsressourcen, die auf der Grundlage der Ähnlichkeit des Zwecks logisch segmentiert sind, und stellt sicher, dass jedes Segment durch Geräte und Dienste (d. h. Web- und Netzwerksicherheits-Gateways, Firewalls usw.), die so konfiguriert und abgesichert sind, dass sie als sicherheitserzwingende Punkte fungieren, getrennt und geschützt ist.

3.3. verwendet in jedem Fall eine starke Verschlüsselung (z. B. FIPS 197), um die Personenbezogenen Daten des Kunden bei der Übertragung oder im Ruhezustand zu schützen.

3.4. setzt, sofern geeignet, Netzwerk- oder Cloud-Schutzkontrollen ein, die in der Lage sind, bösartigen Datenverkehr, der in die Informationsressourcen von Pearson ein- und ausgeht, zu erkennen und zu blockieren.

3.5. entfernt Personenbezogene Daten des Kunden nur dann außerhalb der direkten Kontrolle, wenn der Kunde dies schriftlich genehmigt hat. Wenn dies genehmigt wurde (z. B. im Zusammenhang mit der externen Speicherung von Datensicherungen), dürfen solche Personenbezogenen Daten des Kunden nur auf Geräten transportiert werden, die mit einer vollständigen Festplattenverschlüsselung konfiguriert sind, um die Daten vor Verlust oder Diebstahl zu schützen.

3.6. speichert Personenbezogene Daten des Kunden nicht auf Wechseldatenträgern (z. B. USB-Flash-Laufwerken, USB-Sticks, Speichersticks, Kassetten, CDs oder externen Festplatten) zu speichern, außer: (a) zu Zwecken der Datensicherung, der Geschäftskontinuität, der Wiederherstellung im Katastrophenfall und des Datenaustauschs, wie im Rahmen dieser DSGVO zulässig und erforderlich, und (b) in allen Fällen unter Verwendung einer starken Verschlüsselung.

3.7. stellt sicher, dass alle Pearson-Informationsressourcen gemäß dem Centre for Internet Security Hardening Benchmark (https://www.cisecurity.org/) und/oder dem Sicherheitsleitfaden des Anbieters "abgesichert" sind und bleiben.

4. Sicherheits-Gateways. Pearson:

4.1. fordert für den Verwaltungs- und/oder Management-Zugang zu Sicherheits-Gateways, einschließlich des Zugangs zur Überprüfung von Protokolldateien, eine starke Authentifizierung.

4.2. hat dokumentierter Kontrollen, Richtlinien, Prozesse und Verfahren, eingeführt und nutzt diese, um sicherzustellen, dass unbefugte Benutzer keinen Verwaltungs- und/oder Management-Zugang zu Sicherheits-Gateways haben und dass die Benutzerberechtigungen für die Verwaltung und das Management von Sicherheits-Gateways angemessen sind.

4.3. stellt mindestens alle sechs (6) Monate sicher, dass die Konfigurationen der Sicherheits-Gateways abgesichert sind, indem Sie eine Stichprobe von Sicherheits-Gateways auswählen und überprüfen, ob alle Standardregelsätze und Konfigurationsparameter implementiert sind.

4.4. verwendet Überwachungstools, um zu überprüfen, ob alle Aspekte der Sicherheits-Gateways (z. B. Hardware, Firmware und Software) kontinuierlich einsatzbereit sind.

4.5. konfiguriert und implementiert alle Sicherheits-Gateways so, dass alle nicht betriebsbereiten Sicherheits-Gateways jeglichen Zugang verweigern.

4.6. konfiguriert Echtzeitwarnungen für Änderungen an der Sicherheits-Gateways-Konfiguration und/oder Regelbasis.

5. Identifizierung und Authentifizierung.

5.1. In Bezug auf den Zugang zu den Personenbezogenen Daten des Kunden, entweder in elektronischer Form oder in Papierform, durch das Team von Pearson ist Pearson verpflichtet:

5.1.1. eine starke Authentifizierung (d.h. eine Multi-Faktor-Authentifizierung) für jeden Fernzugriff auf nicht-öffentliche Informationsressourcen zu verlangen.

5.1.2. sicherzustellen, dass der Zugang zu Systemen, die Personenbezogene Daten des Kunden verarbeiten, über einen zentralen Anbieter für Identitätsüberprüfung umgesetzt wird, der den Best Practices der Branche entspricht.

5.1.3. eine sichere Methode für die Übermittlung von Authentifizierungsdaten (z. B. Passwörter) und Authentifizierungsmechanismen (z. B. Token oder Chipkarten) zu verwenden.

5.1.4. gegebenenfalls einen risikobasierten Authentifizierungsmechanismus einführen, so dass die Authentifizierungsmethoden abgestuft sind und in einem angemessenen Verhältnis zur Sensibilität der Personenbezogenen Daten des Kunden stehen, auf die zugegriffen werden soll (d. h. die Verwendung einer stärkeren Form der Authentifizierung für den Zugriff auf Personenbezogene Daten des Kunden)

5.1.5. einen dokumentierten Prozess für die Verwaltung des Lebenszyklus von Benutzer-IDs, einschließlich Verfahren für die genehmigte Einrichtung von Konten, die sofortige Entfernung von Konten bei Kündigung oder innerhalb von 24 Stunden bei Positionswechsel zu haben und anzuwenden und Konten (d. h. Änderungen von Berechtigungen, Zugriffsbereichen, Funktionen/Rollen) für alle Informationsressourcen und in allen Umgebungen (z. B. Produktion, Test, Entwicklung usw.) zu ändern. Dieser Prozess umfasst eine mindestens vierteljährlich durchzuführende Überprüfung der Zugriffsrechte und der Gültigkeit der Konten.

6. Software und Datenintegrität. Pearson:

6.1. stellt sicher, dass alle Computer-, Netzwerk- und Speicherressourcen so konfiguriert sind, dass Sicherheitsfunktionen zur Erkennung, Quarantäne und Verhinderung der Ausführung von bösartigem Code eingesetzt werden.

6.2. trennt die nicht produktions-spezifischen Informationsressourcen von den produktions-spezifischen Informationsressourcen, indem unterschiedliche Computer-, Netzwerk- und Speicherressourcen verwendet werden.

6.3. verwendet nur maskierte Daten in Entwicklungs- und Testumgebungen. Wenn dies nicht möglich ist, muss Pearson die schriftliche Zustimmung des Kunden zur Verwendung nicht identifizierter

Personenbezogener Daten des Kunden einholen, und Pearson garantiert und verpflichtet sich, dass solche Umgebungen über ebenso strenge Zugangskontrollen verfügen, wie die in der Produktion verwendeten.

6.4. verfügt über ein dokumentiertes Änderungskontrollverfahren, einschließlich der Überprüfung der Sicherheitsauswirkungen und der Back-Out-Verfahren für alle Produktionsumgebungen.

6.5. aktiviert bei Anwendungen, die eine Datenbank verwenden, die Änderungen an Personenbezogenen Daten des Kunden ermöglicht, die Funktionen zur Protokollierung von Datenbanktransaktionen und bewahrt die Protokolle der Datenbanktransaktionen mindestens zwölf (12) Monate lang auf.

6.6. überprüft die Software, um alle Sicherheitslücken zu finden und zu beheben (statische, dynamische und Abhängigkeitscode-Analyse), und zwar vor der ersten Implementierung und bei allen Änderungen und Aktualisierungen für alle Software, die im Rahmen einer DPA mit Pearson entwickelt wurde.

6.7. führt Qualitätssicherungsprüfungen durch (unter Verwendung von CREST und/oder eines akkreditierten CHECK-Sicherheitsgutachters) für die Sicherheitskomponenten (z. B. Prüfung der Identifizierungs-, Authentifizierungs-, Autorisierungs-, Vertraulichkeits-, Integritäts-, Verfügbarkeits- und unabweislichen Funktionen) sowie aller anderen Aktivitäten zur Validierung der Sicherheitsarchitektur bei der Erstimplementierung und bei allen Änderungen und Aktualisierungen.

7. Schwachstellen-Scanning und Penetrationstests. Während der Laufzeit dieses AVVs oder während der Verarbeitung Personenbezogener Daten des Kunden durch Pearson (je nachdem, was später eintritt), ist Pearson verpflichtet:

7.1. branchenübliche Tools und manuelle Techniken zur Bewertung der Sicherheit der von Pearson bereitgestellten Lösung(en) zu verwenden.

7.2. mindestens vierteljährlich und unmittelbar nach allen wesentlichen Änderungen und Upgrades einen Schwachstellenscan der externen und internen Informationsressourcen, einschließlich Netzwerken, Servern, Anwendungen und Datenbanken, mit branchenüblicher Software zum Scannen von Sicherheitslücken durchführen, um Sicherheitslücken aufzudecken und sicherzustellen, dass diese Informationsressourcen ordnungsgemäß abgesichert sind.

7.3. mindestens vierteljährlich zu testen, um alle nicht autorisierten drahtlosen Netzwerke zu identifizieren.

7.4. mindestens einmal jährlich einen Penetrationstest durch einen Dritten durchführen zu lassen, der auf Anfrage per Bildschirmfreigabe geteilt wird. Werden bei diesen Tests Schwachstellen festgestellt, stellt Pearson rechtzeitig ausreichend technisch geschultes Personal und Unterstützung zur Verfügung, um die festgestellten Probleme zu beheben und weitere ethisch vertretbare Hacks durchzuführen, bis der Kunde sicher ist, dass die festgestellten Vorfälle und die ihnen zugrunde liegenden Ursachen behoben wurden.

8. Protokollierung. Pearson:

8.1. protokolliert privilegierte Konten auf allen Geräten und Anwendungen.

8.2. protokolliert Zugriffs- (Lese-), Schreib-, Änderungs- und Anmeldeversuche, fehlgeschlagene Zugriffsversuche, Änderungen an Zugriffskontrolllisten, Identifikatoren oder Gruppen-/Rollenprivilegien, Aktualisierungen von Sicherheitssoftware oder der Funktionalität von Software und Anwendungen sowie die Ausführung von Programmen, die Zugriffskontrollen umgehen können.

8.3. implementiert einen Echtzeit-Protokollierungsserver und beschränkt den Zugriff auf Sicherheitsprotokolle auf befugte Personen und schützt die Sicherheitsprotokolle vor unbefugten Änderungen und bietet ein zentrales Mittel zur Überwachung der Sicherheitsprotokolle. Alle Sicherheitsprotokolle und sicherheitsrelevanten Audit-Protokolle sind mindestens wöchentlich auf Anomalien zu überprüfen und alle protokollierten Sicherheitsprobleme zeitnah zu beheben.

8.4. bewahrt alle Sicherheits- und Serverprotokolle für einen Zeitraum von einem Jahr auf (mit einer Online-Verfügbarkeit von 90 Tagen) oder so lange, wie es für die Einhaltung gesetzlicher Vorschriften erforderlich ist, je nachdem, welcher Zeitraum länger ist. Das Protokoll zeichnet alle logischen Zugriffsversuche auf, sowohl gültige als auch ungültige. Das Protokoll enthält den Namen (ID), Datum und Uhrzeit der Anmeldung, die Datensätze, auf die zugegriffen wurde, und die durchgeführte Aktivität. Wenn möglich, enthält das Protokoll auch einen Eintrag für die Abmeldung.

9. Physische Sicherheit. Pearson:

9.1. stellt sicher, dass alle Systeme, die zur Verarbeitung und Speicherung Personenbezogener Daten von Kunden verwendet werden, in sicheren, überwachten und zugangskontrollierten Räumlichkeiten untergebracht sind;

9.2. bringt alle Informationsressourcen in sicheren, gehosteten Einrichtungen, zu denen nur befugte Personen Zugang haben unter;

9.3. bringt alle Informationsressourcen in Gegenden unter, die einen angemessenen Rechtsrahmen bieten, um die Einhaltung der Bedingungen dieses AVVs zu gewährleisten;

9.4. überwacht und zeichnet den Zugang zu den physischen Einrichtungen auf, in denen Informationsressourcen untergebracht sind, die von mehreren Nutzern verwendet werden sollen, zu Prüfzwecken, einschließlich des Namens des Mitarbeiters, der Uhrzeit und des Datums des Betretens und Verlassens, und überwacht, sofern möglich, den Raum durch eine Kamera.

10. Mobile und portable Geräte. Pearson:

10.1. überprüft mindestens einmal jährlich die Nutzung und die Kontrollen aller von Pearson verwalteten oder betreuten mobilen und portablen Geräte, um sicherzustellen, dass die mobilen und portablen Geräte die geltenden Anforderungen an die Informationssicherheit erfüllen können.

10.2. Drahtlose Vernetzung. Wenn der Kunde schriftlich zustimmt, stellt Pearson bei der Verwendung von auf Funkfrequenzen (RF) basierenden drahtlosen Netzwerktechnologien zur Erbringung oder Unterstützung von Diensten für den Kunden sicher, dass alle übertragenen Personenbezogenen Daten des Kunden durch den Einsatz geeigneter Verschlüsselungstechnologien geschützt werden, die ausreichen, um die Vertraulichkeit der Personenbezogenen Daten des Kunden zu wahren. Die Verwendung von RF-basierten drahtlosen Headsets, Tastaturen, Mikrofonen und Geräte zum Zeigen, wie Mäusen, Touchpads und digitale Zeichentabletts, ist von dieser Anforderung ausgenommen.