Technische und organisatorische Maßnahmen (TOM) zur Gewährleistung des Datenschutzes bei der Lernverlaufsdiagnostik quop i.S.d. Art. 32 Datenschutz-Grundverordnung (DSGVO)

hfp hauser, furch & partner
Informationssysteme GmbH

INHALTSVERZEICHNIS

ANSPRECHPARTNER

Dipl.-Ing. Ulrich Mayer
E-Mail: ulrich.mayer@hfp.de
Telefon: 06190 – 888 35 207

Wirtsch.-Ing. (M.Sc.) Johannes Köpf
E-Mail: johannes.koepf@hfp.de
Telefon: 06190 – 888 35 211

hfp Informationssysteme GmbH
Philipp-Reis-Str. 2
65795 Hattersheim
Telefon: 06190 – 888 35 0
E-Mail: hfp@hfp.de
Internet: www.hfp.de

Für die Durchführung im Land Niedersachsen:

Niedersächsisches Kultusministerium:

Hr. Ralf Borngräber (Ref. 25)

Herr Peter Reinert (Ref. 32)

Niedersächsisches Landesinstitut für schulische Qualitätsentwicklung:

Fr. Laura Hempel (FB 33)

Keßlerstraße 52

31134 Hildesheim

Telefon: 05121 1695-204

E-Mail: laura.hempel@nlq.niedersachsen.de

Technische und organisatorische Maßnahmen (TOM) zur Gewährleistung des Datenschutzes bei der Lernverlaufsdiagnostik quop i.S.d. Art. 32 DSGVO

- Version: 1.0 Januar 2014
- Version: 1.1 August 2015
- Vorgelegt beim Datenschutzbeauftragen des Landes Hessen im Dezember 2017

- Version: 1.2 Aktualisiert September 2018
- Version 1.3 Vorgelegt beim Niedersächsischen Landesinstitut für schulische Qualitätsentwicklung (NLQ), Dezember 2020
- Version 1.4 Vorgelegt beim Niedersächsischen Landesinstitut für schulische Qualitätsentwicklung (NLQ), Januar 2021
- Version 1.5 Vorgelegt beim Niedersächsischen Landesinstitut für schulische Qualitätsentwicklung (NLQ), Januar 2021

1 Name und Anschrift der datenverarbeitenden Stelle

1.1. Name und Anschrift

Niedersächsisches Kultusministerium

Hans-Böckler-Allee 5

30173 Hannover

1.2. Organisationskennziffer, Amt, Abteilung, ggf. Sachgebiet

Niedersächsisches Kultusministerium

Niedersächsisches Landesinstitut für schulische Qualitätsentwicklung (NLQ)

1.3. Name und Anschrift des Auftragnehmers, wenn die Daten gem. Art. 28 DSGVO im Auftrag verarbeitet werden

hfp Informationssysteme GmbH

Innovationspark

Philipp-Reis-Str. 2

65795 Hattersheim

2 Zweckbestimmung der Lernverlaufsdiagnostik quop

Die internetbasierte Lernverlaufsdiagnostik mit quop basiert auf einer Reihe von Erkenntnissen aus Forschung und Praxis. Das Verfahren quop erfasst nach dem Konzept des formativen Assessments die Leistungsentwicklung von Schüler/innen in kurzen zeitlichen Abständen in den zentralen Leistungsbereichen Lesen (Klassenstufe 1 bis 6), Mathematik (Klassenstufe 1 bis 6) und Englisch (Klassenstufe 5 bis 6) am Computer.

Die auf den Lernverlauf ausgerichtete Diagnostik verfolgt das Ziel, Lehrkräften eine große, verlässliche Informationsbasis zur Anpassung und Optimierung des Lernprozesses *während* des Schuljahres bereitzustellen. Lehrkräfte erhalten fortlaufend Informationen über die tatsächlichen Kompetenzen einzelner Schüler/innen oder der ganzen Klasse und können darauf angemessen reagieren, z. B. auch indem sie Instruktionsanpassungen vornehmen, sofern die Lernverläufe dies nahelegen.

Bei quop handelt es sich um ein gut erforschtes Verfahren zur Lernverlaufsdiagnostik. Alle in quop zur Verfügung gestellten Testverfahren wurden oder werden im Hinblick auf die zentralen psychometrischen Gütekriterien umfassend analysiert und optimiert. Darüber hinaus wird quop selbst konsequent wissenschaftlich evaluiert und weiterentwickelt.

2.1. Bezeichnung des Verfahrens

quop. Die Lernverlaufsdiagnostik.

2.2. Rechtsgrundlage

- § 54 Abs. 1, Niedersächsisches Schulgesetz (NSchG): Recht auf Bildung; begabungsgerechte individuelle Förderung.
- § 31, Abs, 1, Niedersächsisches Schulgesetz (NSchG): Verarbeitung personenbezogener Daten zur Erfüllung des Bildungsauftrags der Schule; zur Erforschung oder Entwicklung der Schulqualität.
- § 31, Abs, 5, Niedersächsisches Schulgesetz (NSchG): Einsatz Internetbasierte Lern- und Unterrichtsplattformen.
- § 31, Abs, 10, Niedersächsisches Schulgesetz (NSchG): Verarbeitung der Schülerstammdaten einschließlich der optionalen Felder „Migrationshintergrund“ und „sonderpädagogischer Förderbedarf“.
- **Art. 32 DSGVO (Sicherheit der Verarbeitung)**

3 KREIS DER BETROFFENEN

- Lehrkräfte, sofern sie sich für die Teilnahme an quop anmelden. Zunächst sind das insbesondere Mitarbeitende am Projekt "Lesen macht stark Niedersachsen", sofern sie sich für die Teilnahme an quop anmelden.
- Schüler/innen, sofern die Klasse von der Lehrkraft für quop angemeldet wird.

4 Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

4.1. Herkunft der Daten	4.2. Art der Daten	4.3. Empfänger der Daten
Erfassung durch Lehrkräfte oder technische Administratoren des Verfahrens	Schulen: Name, Adresse, Telefonnummer, E-Mail-Adresse, Nachname, Vorname und E-Mail-Adresse der Schulleiterin/des Schulleiters	- Lehrkräfte - Administratoren
Erfassung durch Lehrkräfte oder technische Administratoren des Verfahrens	Lehrkräfte: Name, Vorname, E-Mail-Adresse, Klasse-Fach-Kombinationen in denen quop genutzt werden soll Lehrkräfte optional[1]: Bereitschaft zu wissenschaftlicher Mitarbeit (ja/nein), Telefonnummer sowie freiwillige Angaben	- Lehrkräfte - Administratoren
Erfassung durch Lehrkräfte	Schüler/innen[2]: Name, Vorname, Passwort, zugeordnete Testreihe (Fach und Stufe), Geschlecht, Geburtstag, Sonderpädagogischer Förderungsbedarf (ja/nein), Migrationshintergrund (ja/nein), Einschulungsjahr	Nur die jeweils für die Schülerin/den Schüler zuständige Lehrkraft
Automatisierte Auswertung nach der Bearbeitung von Testaufgaben durch Schüler/innen	Schüler/innen: Lernstand in Lesen und/oder Mathematik und/oder Englisch	Schüler/innen (nur die eigenen Lernverlaufskurven) Lehrkräfte erhalten alle diagnostischen Auswertungen der Schülerinnen und Schüler

[1] Diese Angaben können ohne Auswirkungen auf die weitere Programmbearbeitung übersprungen werden.

[2] In Niedersachsen werden im Projekt des NLQ keine personenbezogenen Daten der Schülerinnen/Schüler erfasst.

5 Zugriffsberechtigte Personen oder Personengruppen

Zugangsberechtigt sind:

1. Lehrkräfte ausschließlich für die ihnen zugeordneten Schüler/innen und deren Tests und Testergebnisse
2. Schüler/innen ausschließlich für die ihnen zugeordneten Tests
3. Administratoren des Verfahrens für Lehrkräfte und Schulen sowie Testvorlagen, pseudonymisierte Verlaufsdaten

6 Technische und organisatorische Maßnahmen

6.1. Zutrittskontrolle

Die quop-Server selbst stehen in einem Sicherheitsrechenzentrum mit mehrfacher Zutrittskontrolle, personenbezogener, biometrischer Identifizierung und kontinuierlicher Videoüberwachung (24 Stunden an 7 Tagen der Woche). Zusätzlich sind die Server gegen Manipulation von außen in Schränken eingeschlossen. Gegen elektronische Angriffe werden die Server mit ständig aktuellen softwaretechnischen Maßnahmen mehrfach abgesichert.

6.1.1 Technische Absicherung

- Alle Räume sind mit Alarmanlagen gegen Einbruch, Wasser und Brand abgesichert.
- Alle Räume sind durch automatische Zugangskontrollsysteme mit Einpersonen-Schleusen zusätzlich abgesichert.
- Der Zugang wird durch biometrische Zugangssperren nämlich Fingerabdruck-Scanner gesichert.
- Die Server selbst sind in fest installieren Käfigen durch manuelle Schließsysteme mit Sicherheitsschlössern gesichert.
- Das Gebäude ist umzäunt, videoüberwacht und durch Wachpersonal geschützt.
- Es gibt keine frei zugänglichen Gebäudeschächte oder unbewachten Zutrittsmöglichkeiten auf das Gelände oder zu den Anlagen.

6.1.2 Organisatorische Absicherung

- Es gibt eine Schlüsselregelung, nach der nur drei ausgewiesene Personen überhaupt Zutritt zu den Servern haben.

- Der Empfang ist immer (7x24) mit Sicherheitspersonal besetzt. Das Sicherheitspersonal führt zwingend Personenkontrollen an abgeriegelten Schleusen durch. Die Vorlage des Personalausweises und der Abgleich mit der Liste autorisierter Personen ist zwingend. Jeder Besuch wird protokolliert und zusätzlich videotechnisch aufgezeichnet.
- Autorisierte Besucher erhalten temporäre Besucherausweise, die nach dem Besuch zurückgegeben werden und gelöscht werden müssen.
- Nicht autorisierte Besucher können ausschließlich in Begleitung autorisierter Besucher das Rechenzentrum betreten. Nicht autorisierte Besucher können sich nur in Begleitung innerhalb des Rechenzentrums bewegen.

6.2. Zugangskontrolle zu den Servern

6.2.1 Technische Maßnahmen

- Die quop-Server sind durch Firewalls geschützt.
- Alle Zugangspassworte sind „echte Passwörter“, das heißt sie bestehen aus mindestens 8 Buchstaben, zufallsgenerierten Zeichenfolgen mit Buchstaben, Zahlen und Sonderzeichen.
- Die Server sind redundant ausgelegt und stehen in unterschiedlichen Hallen, um gegen Elementarschäden (Feuer, Wasser, etc.) abgesichert zu sein.

6.2.2 Organisatorische Absicherung

- Nur ausgewählte, sicherheits- und datentechnisch belehrte Personen haben die Zugangsmöglichkeiten zu den quop-Servern.
- Der physische Zugang ist nur durch personenidentifizierende Eingangskontrollen möglich.
- Ein Remote-Zugang ist ausschließlich über abgesicherte VPN-Zugänge und durch speziell autorisierte Mitarbeiter möglich.

6.3. Benutzerkontrolle

6.3.1 Lehrkräfte

Im Anwenderbereich erfolgt die Benutzerkontrolle passwortgeschützt. Der Login erfordert die E-Mail-Adresse der Lehrkraft und ein Passwort

- Die Schulen der Lehrkräfte werden durch das Niedersächsische Kultusministerium, NLQ authentifiziert.

- Das Startpasswort wird den Lehrkräften an die persönliche E-Mail-Adresse zugestellt.
- Passwörter müssen aus mindestens 8 Zeichen bestehen und mindestens einen Großbuchstaben, mindestens einen Kleinbuchstanden, eine Zahl und ein Sonderzeichen enthalten.

Die Lehrer-Clients sind per selbstgewähltem Passwort gesichert.

6.3.2 Schüler

Der Login erfordert den Schülernamen und ein Passwort.

- Die zugangsberechtigten Schüler werden durch die Lehrkräfte authentifiziert.
- Das Startpasswort für die Schüler wird automatisch generiert und den Lehrkräften bereitgestellt.
- Die Anforderungen an die Passwörter entsprechen denen für Lehrkräfte
- Alle eingegebenen Schülerdaten werden on-the-fly pseudonymisiert und pseudonymisiert abgelegt.

Nur die Lehrkraft kann die Schülerdaten im Lehrerclient flüchtig decodieren, so dass ausschließlich die Lehrkraft oder von der Lehrkraft autorisierte andere Lehrkräfte die Klarnamen[3] der Schüler sehen können.

6.4. Zugriffskontrolle

Mit dem Passwort kann nur auf die Daten zugegriffen werden, für die ein Benutzer mit seinem Login autorisiert ist.

6.5. Datenverarbeitungskontrolle

Um schon softwareseitig höchstmöglichen Schutz zu bieten, werden die personenidentifizierenden Daten[4] der Schüler/innen bei der Anlage in quop bei der Erfassung pseudonymisiert und verschlüsselt und auch nur verschlüsselt unter dem Pseudonym abgespeichert.

Nach der Anlage der Schüler/innen im quop-System werden die personenidentifizierenden Daten im Klartext nur für autorisierte Personen (d.h. nur die zuständige Lehrkraft) temporär sichtbar gemacht. Dies geschieht beim Zugriff auf die Schülerdaten, bei dem die Daten auf dem Server flüchtig mit dem Passwortschutz decodiert werden.

[3] In Niedersachsen werden im Projekt des NLQ keine Klarnamen der Schülerinnen und Schüler verwendet.

[4] In Niedersachsen werden im Projekt des NLQ keine personenidentifizierenden Daten der Schülerinnen und Schüler verwendet.

6.6. Verantwortlichkeitskontrolle

Nur autorisierte Personen (zuständige Lehrkräfte) können personenbezogene Schülerdaten verarbeiten.

Alle anderen zugriffsberechtigten Personen können pseudonymisierte Schülerdaten verarbeiten oder Daten ohne Personenbezug.

6.7. Organisatorische Absicherung

Mit den personenbezogenen Daten der Schüler/innen kommt nur autorisiertes oder dem niedersächsischen Datenschutz unterstelltes Personal – insbesondere die Lehrkräfte - in Berührung.

Mit allen Mitarbeitern bei hfp sind entsprechende datenschutzrechtliche Regelungen vertraglich vereinbart. Die Mitarbeiter werden regelmäßig datenschutzrechtlich belehrt.

6.8. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO; Art. 25 Abs. 1 DSGVO)

Alle eingegebenen Schülerdaten[5] werden on-the-fly pseudonymisiert und pseudonymisiert abgelegt. Nur die Lehrkraft kann die Schülerdaten im Lehrerclient flüchtig decodieren, so dass ausschließlich die Lehrkraft oder von der Lehrkraft autorisierte andere Lehrkräfte die Klarnamen der Schüler sehen können. In den Datenbanken liegen ausschließlich Pseudonyme.

7 TECHNIK DES VERFAHRENS

Computerbasierte Verfahren für die Schule müssen für die dort vorzufindenden Rahmenbedingungen geeignet sein. Schulcomputer haben in der Regel keinen einheitlichen technischen Standard und sehr unterschiedliche Nutzungszeiträume, es werden zum Teil auch sehr alte Geräte und sehr uneinheitliche Wartungs-, Sicherheits- und Pflegekonzepte vorgefunden, und nicht zuletzt setzen Schulen Hardware mit sehr unterschiedlichen Betriebssystemen ein. Auf der anderen Seite kommen vermehrt z. B. auch iPads zum Einsatz.
Der quop-Client nutzt keine veralteten Browserversionen oder Ausgabekomponenten wie den Adobe Flash Player.

[5] In Niedersachsen werden im Projekt des NLQ keine personenidentifizierenden Daten der Schülerinnen und Schüler verwendet.

7.1. quop ist eine web-basierte Anwendung

Sowohl Lehrkräften als auch Schüler/innen wird quop als eine in einem Browser lauffähige Anwendung über das Internet bereitgestellt. Dies hat zum einen den Vorteil, dass keine Installation von Software auf den Arbeitsplatzrechner bzw. Tablets in den Schulen notwendig ist. Zum anderen können Updates zentral bereitgestellt werden, so dass alle teilnehmenden Lehrkräfte und Schüler/innen unmittelbar von kontinuierlichen technischen Weiterentwicklungen profitieren.

Für die Audio-Ausgaben, die für einige Testinstruktionen und Aufgaben benötigt werden, wird keine zusätzliche Software benötigt, wie z.B. den Adobe Flash Player.

Das Verfahren quop läuft auf Arbeitsplatzrechnern, Tablets sowie Smartphones mit den gängigsten Betriebssystemen: Windows, IOS, Linux, Android.

Die Daten werden lediglich im Browser angezeigt. Alle aufwändigen Operationen werden auf dem Server ausgeführt. Weil die Ressourcen der Arbeitsplatzrechner bzw. Tablets nahezu nicht belastet werden, ist eine performante Lauffähigkeit auch auf alten und schwachen Systemen gesichert, gleichzeitig belastet quop auch die Internetverbindungen nur sehr geringfügig.

7.2. Gewährleistung des Datenschutzes durch Mehrebenen-Verschlüsselung und Pseudonymisierung

Zur Gewährleistung des Datenschutzes werden die Daten zwischen den Clients und dem Server über das sichere Hypertext-Übertragungsprotokoll https übertragen. Für die Administratoren und das quop-Serviceteam erfolgt die Datenanzeige pseudonymisiert. Eine Rückverfolgung auf einzelne Schüler/innen ist damit nicht möglich. Sollte eine Kommunikation mit Lehrkräften über konkrete Schüler/innen im Rahmen fachlicher Unterstützung erforderlich sein, so erfolgt diese ausschließlich mit der individuellen Schüler-ID.

Die Speicherung der personenbezogenen Daten in der Datenbank erfolgt ebenfalls pseudonymisiert. Der Server des quop-Verfahrens wird zudem in einem Hochsicherheitsrechenzentrum mit biometrisch abgesicherter Zugangskontrolle betrieben.

Die Datenübertragung und die Datenablage erfolgt echtzeitverschlüsselt mit dem asymmetrischen kryptographischen RSA Verfahren mit 15.360 Bit und wird mit dieser Verschlüsselung auf den Festplatten abgelegt. Die Zugangskontrolle erfolgt für wenige legitimierte Personen über biometrische Daten. Unabhängig von diesen technischen Sicherungen des Datenschutzes unterliegen alle an quop beteiligten Personen dem Datenschutz.

7.3. Massentaugliche Softwarearchitektur und leistungsfähige Internetanbindung

Anwendungen, die auf zentralen Servern laufen und bei denen viele Nutzer gleichzeitig auf ein System zugreifen, müssen diesen Zugriffen standhalten. Hierzu sind eine schnelle Internetanbindung und eine massentaugliche Softwarearchitektur erforderlich. Über beides verfügt quop. Das quop-Verfahren ist über eine Gigabit-Leitung mit zentralen Internet-Knotenpunkten in Deutschland und Europa verbunden und damit quasi an das ‘Internet-Backbone‘ angeschlossen. Unser Rechenzentrum verfügt über 740 GBit/s private Peerings, ein Peering mit der Deutschen Telekom (120 GBit/s) und einer 100 GBit/s-Anbindung an das DE-CIX in Frankfurt. Der Zugang zum Internet-Backbone ist in Deutschland in nur wenigen Rechenzentren verfügbar. So ist eine sehr gute Erreichbarkeit des quop-Verfahrens gegeben.

quop stellt sicher, dass möglichst wenig Datenverkehr zwischen den Anwendern und dem quop-Server stattfindet, um optimale Performanz zu gewährleisten.

Die quop-Server sind Eigentum der hfp Informationssysteme GmbH.

7.4. Umgebungsunabhängige Stabilität der Messergebnisse

Je nach Leistungsfähigkeit der Internetanbindung einzelner Schulen und der Nutzung durch Schüler/innen und Lehrkräfte kann es während der Durchführung eines Tests zu Schwankungen in den Netzlaufzeiten aufgrund schwacher Anbindungen an das Internet kommen. Durch diese Verzögerungen wird die Messung der Bearbeitungszeiten je Test jedoch nicht verfälscht, da in die Messung immer nur die tatsächlich benötige Bearbeitungszeit eingeht.

7.5. Hohe Verfügbarkeit aufgrund redundanter Systeme

Das Verfahren quop wird mit einer hohen Verfügbarkeit bereitgestellt und betrieben. Im unwahrscheinlichen Fall eines technischen Ausfalls in der Server-Infrastruktur steht innerhalb von zwei bis vier Stunden ein redundantes System für die Fortsetzung des Betriebs bereit. Die Datenlage dieses redundanten Systems entspricht dem Zustand unmittelbar vor dem technischen Ausfall. Das bedeutet unter anderem, dass im unwahrscheinlichen Fall eines technischen Ausfalls die aktuelle Datenlage schnell wiederhergestellt werden kann.

8 Löschfristen

Eine Lehrkraft kann die personenbezogenen Schülerdaten (insbesondere Lernverlaufskurven) nur solange einsehen, wie die Schülerin/der Schüler dieser Lehrkraft zugeordnet ist. In der Regel werden die personenbezogenen Schülerdaten nach zwei Jahren gelöscht.

Die personenbezogenen Daten einer Lehrkraft werden nur für die Dauer der Tätigkeit beim Niedersächsischen Kultusministerium gespeichert und anschließend zeitnah gelöscht.

Angestrebt ist die Löschung aller personenbezogenen Daten nach dem Projektende von "Lesen macht stark" 2023, ggf. wird 2024 evaluiert und diese Daten werden spätestens 2024 gelöscht.

9 Datenübermittlung in Staaten außerhalb der Europäischen Union

Eine Datenübermittlung in Staaten außerhalb der Europäischen Union findet nicht statt.