ENSECUR

DATENSCHUTZ
BESSER
MACHEN

DATENSCHUTZ BEI ONLINE UNTERRICHT

White Paper

erstellt von der ENSECUR GmbH

Version 1.03

Stand: 10.07.2020

ENSECUR GmbH

Standort Karlsruhe:
Kaiserstraße 86
76133 Karlsruhe
T: +49 (0) 721/180 356 70
F: +49 (0) 721/180 356 75

Standort Stuttgart:
Sophienstraße 25
70178 Stuttgart
T: +49 (0) 711/460 541 40
F: +49 (0) 711/460 541 45

Registergericht Mannheim
HRB 712239
USt-ID-Nr. DE277945684
Mail: info@ensecur.de
Web: www.ensecur.de

Geschäftsführer
Julian Häcker
Thorsten Jordan

ENSECUR DATENSCHUTZ BESSER MACHEN

Inhaltsverzeichnis

1 Motivation und Nutzen

Die Digitalisierung an Schulen ist eines der zentralen Zukunftsthemen in Deutschland. Mit dem DigitalPakt Schule wollen Bund und Länder die Digitalisierung an Schulen vorantreiben. Die Corona-Pandemie beschleunigte unfreiwillig diese Bestrebungen. Zwar startet der Unterricht in einzelnen Bundesländern mit den Abschlussklassen zum 04. Mai 2020, jedoch liegen zu diesem Zeitpunkt bereits herausfordernde Wochen ohne Präsenzunterricht hinter Schülern und Lehrkräften.

In der Zwischenzeit übernahmen viele Eltern neben der eigenen Berufstätigkeit aus der Not heraus auch die Funktion von Hilfs-Lehrkräften. Sie mussten feststellen, welche Zusatzbelastung das bedeutet und die Leistung der Lehrkräfte ihrer Kinder fand eine völlig neue Anerkennung. Aufgrund der Doppelbelastung wünschen sich viele Eltern mehr Unterstützung durch Lehrkräfte bei der Fortführung des Unterrichts in Zeiten von Corona. Ein reines Aufgaben per E-Mail zuschicken und später nach Bearbeitung zurückschicken sei zu wenig.

Die Rufe nach weiterer Unterstützung in Form von Videounterricht, Kommunikation per Messenger oder über Schulplattformen wurden lauter. In Presseartikeln äußerten erboste Eltern ihren Unmut über rückständige Schulen und Lehrkräfte. Motivierte Lehrkräfte reagierten, dass sie ja gerne helfen würden, jedoch strenge Vorgaben seitens des Kultusministeriums oder des staatlichen Schulamts hätten und dass die Vorgaben zum Datenschutz eingehalten werden müssten. In vielen Fällen gab es keine konkreten Empfehlungen für digitale Werkzeuge seitens des Kultusministeriums, stattdessen verwiesen diese auf die Zuständigkeit der Schulen. Viele Schulen verfügen jedoch nicht über die Expertise und die Ressourcen, die digitalen Werkzeuge so zu bewerten bzw. so zu konfigurieren, dass sie diese mit gutem Gewissen und unter Beachtung der gesetzlichen Vorgaben kurzfristig einsetzen können.

Aus der Not heraus bzw. aufgrund des Drucks erboster Eltern griffen Lehrkräfte kurzerhand zu digitalen Helfern. In vielen Fällen ist die IT der Schulen nicht im Boot, Datenschutzbeauftragte außen vor und somit sind diverse gesetzlichen Anforderungen nicht berücksichtigt. Als dann Stimmen laut wurden, dass Datenschutzanforderungen die Digitalisierung an Schulen ausbremsen und auch Online Unterricht verhindern würde, wussten wir, dass es Zeit war zu reagieren:

Wir wollen mit diesem Whitepaper Lehrkräften Hilfestellung für konkrete Fragestellungen bieten. Im Fokus stehen Videokonferenztools, der Einsatz von Messenger Apps, Tipps zum Home-Office / Home- Schooling und Hinweise zum sicheren Datenaustausch zwischen Lehrkräften und Schülern sowie Schulplattformen.

Da wir im Rahmen unserer Datenschutzberatung auch Klienten mit schulischen Angeboten betreuen, kennen wir die eine oder andere Anforderung von Lehrern. Teilweise sind wir selbst Eltern und Lehrende und erleben die Herausforderungen, denen sich Lehrkräfte und Eltern stellen müssen.

Ziel dieses Whitepapers ist es, Lehrkräften und Schulen sowie Eltern, Sicherheit beim Online Unterricht zu geben. Wir wollen dazu beitragen, dass die Digitalisierung des Unterrichts nicht durch den Datenschutz verhindert, sondern von diesem sicher flankiert wird. Da wir uns primär an Lehrkräfte richten, mögen uns geschätzte Kollegen die ein oder andere Reduzierung auf das Wesentliche für Lehrkräfte verzeihen. Maskuline Formen schließen feminine Formen in diesem Text stets mit ein. Mit *Lehrer* sind also auch gleichzeitig *Lehrerinnen* gemeint.

2 Home-Office / Home-Schooling

2.1 Was Sie beim Arbeiten zu Hause beachten sollten

Die Privatwohnung erfüllt in der Regel nicht die gleichen Sicherheitsstandards, wie es in der Schule der Fall ist. Daher besteht ein erhöhtes Missbrauchsrisiko von Daten durch Dritte, welches durch die folgenden Praxishinweise reduziert werden kann. Sie als Lehrer stehen im Home-Office umso mehr in der Verantwortung, die Daten angemessen vor Verlust, Zugriff oder Einsichtnahme durch Unbefugte zu schützen, da Sie sich nicht im „*Schutzraum Schule*“ befinden.

2.1.1 Praktische Umsetzung der Datensicherheit im Home-Office

	Wichtige Anforderungen aus Sicht des Datenschutzes			
	Anforderung	**Erläuterung**	**Erfüllt Ja**	**Nein**
1	**Unbefugte Einsichtnahme verhindern**	Achten Sie darauf, dass keine Unbefugten Einsicht in personenbezogene Daten nehmen und auch bei Videokonferenzen nicht mithören können. *„Unbefugte“* sind in diesem Kontext auch Kinder, Ehepartner oder sonstige im Haushalt lebende Personen. Es bietet sich also an, in einem geschlossenen separaten Zimmer zu arbeiten und ggf. Kopfhörer zu verwenden.		
2	**Offizielle Ausrüstung verwenden**	Grundsätzlich sollten Sie im Home-Office nur mit den von der Schule bereitgestellten betrieblichen Geräten und Softwareanwendungen arbeiten. Nutzen Sie Schulgeräte nur für dienstliche Zwecke.		
3	**Sichere Einwahl auf das Schulnetzwerk**	Greifen Sie auf das Netzwerk der Schule am besten nur über eine gesicherte Verbindung (VPN) zu.		
4	**Eigenes Netzwerk absichern**	Stellen sie sicher, dass der häusliche WLAN-Router mit der aktuell höchsten Sicherheitsstufe konfiguriert (WPA2 Sicherheitsstandard) und der WLAN-Zugang durch ein komplexes Passwort geschützt ist (Anmerkung: Tipps zu sicheren Passwörtern am Ende dieser Tabelle!). → Dies können Sie i.d.R. in den Einstellungen Ihres Routers unter Sicherheit konfigurieren. Denken Sie daran, das vorgegebene Passwort, welches auf der Unterseite des Routers steht, unbedingt zu ändern.		
5	**Zugriff auf Computer schützen**	Schützen Sie den Zugang zum Computer mit einem komplexen Passwort. Sperren Sie beim Verlassen des Arbeitsplatzes das Gerät, so dass bei der Rückkehr zum		

	Wichtige Anforderungen aus Sicht des Datenschutzes			
	Anforderung	**Erläuterung**	**Erfüllt Ja**	**Nein**
		Arbeitsplatz die erneute Eingabe des Passwortes erforderlich ist. → Tastenkombination „Strg“+“Alt“+“Entf“ oder „Windows-Taste“+ „L“ gleichzeitig drücken! Stellen Sie das Gerät so ein, dass die automatische Sperrung nach 5 Minuten erfolgt, falls Sie die manuelle Sperrung einmal vergessen sollten. → Über Energieoptionen ist einstellbar, ab wann eine Sperrung erfolgt. Fahren Sie das Gerät am Ende des Arbeitstages herunter, da ein Angreifer auch bei einer Verschlüsselung im Ruhemodus das Gerät angreifen kann. Bewahren Sie den Computer sowie sonstige Unterlagen in einem abschließbaren Schrank auf. Entfernen Sie im privaten Gebrauch befindliche und genutzte Sprachassistenzsysteme (z.B. ALEXA etc.) aus dem Home-Office. Denn ALEXA hört mit!		
6	**Private Geräte schützen**	Sofern Sie doch auf einem privaten Gerät arbeiten, so beachten Sie bitte die Sicherheitshinweise Ihrer Schule. Verschlüsseln Sie die Festplatte Ihres PC/Laptops (z.B. mit VeraCrypt oder Bitlocker) →Anleitung zum Verschlüsseln mit VeraCrypt z.B. auf dem Portal Lehrerinnenfortbildung Baden-Württemberg oder über dieses Video		

Tipps für sichere Passwörter:

- Ihr Passwort sollte komplex sein: Mindestlänge 12 Zeichen; Verwendung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (3 aus 4 Kriterien).
- Halten Sie so wenige Passwörter wie möglich schriftlich fest und bewahren Sie sämtliche Passwörter an einem sicheren Ort auf, z.B. in einem abgeschlossenen und sicheren Schrank oder in einem entsprechenden Programm auf dem Computer wie dem Passwortsafe „KeePass“ (https://keepass.info/). Das Zugangspasswort zum Passwortsafe sollten Sie sich nicht aufschreiben, sondern merken!
- Damit Sie sich komplexe Passwörter leichter merken können, bilden Sie einen Merksatz und übernehmen Sie die Anfangsbuchstaben. Beispiel: Klaus isst um 13 Uhr eine Pizza mit 4 Zutaten. -> Passwort: Kiu13UePm4Z.
- Nutzen Sie jedes Passwort nur einmal und nutzen Sie insbesondere keine Passwörter, die Sie auch im privaten Gebrauch verwenden.

2.1.2 Besondere Vorsicht bei der Nutzung privater Endgeräte

Wie bereits oben erläutert, sollten Sie ausschließlich betriebliche Geräte nutzen. Sollte für Sie dennoch die Nutzung von privaten Laptops, Rechnern oder Smartphones relevant werden, so berücksichtigen Sie bitte zusätzlich die folgenden spezifischeren Maßnahmen zur Datensicherheit:

- Stellen Sie sicher, dass auf dem privaten Computer bzw. dem privaten Smartphone stets die aktuellste Version des Betriebssystems installiert ist.
- Alle vom Hersteller verfügbaren Sicherheitspatches, Updates und Upgrades sollten Sie unverzüglich installieren.
- Verwenden Sie ausschließlich aktuelle Browser mit den neusten Aktualisierungen.
- Stellen Sie sicher, dass stets ein aktueller Virenschutz aktiv ist.
- Von einer lokalen Speicherung personenbezogener Daten sollten Sie möglichst absehen. Eine Speicherung in einer privaten Cloud ist nicht zulässig.
- Wenn ein Datentransfer vom privaten Endgerät auf das dienstliche Endgerät per mobilem Datenträger erfolgt (USB-Sticks, externe Festplatten), sollten Sie die Datenträger (wenn möglich) zuvor durch die IT auf Viren untersuchen lassen.
- Grundsätzlich sollten Sie nur mobile Datenträger verwenden, die durch die IT ausgegeben werden.
- Vermeiden Sie eine Vermischung von betrieblichen und privaten Daten.
- Schließen Sie private Anwendungen während Sie dienstliche Anwendungen verwenden.
- Nutzen Sie möglichst keine „*Familien-PCs*“ bzw. keine Familienkonten. Es bietet sich also an, ein separates Gerät oder ein extra passwortgeschütztes Konto für den dienstlichen Kontext auf dem „*Familien-PC*“ zu verwenden. Familienmitglieder dürfen keinen Zugang zu personenbezogenen Daten erhalten, insbesondere auch nicht auf gespeicherte Daten. Ein passwortgeschütztes Konto auf einem gemeinschaftlich genutzten Computer können Sie so einrichten:
  Für Windows 10 klicken Sie hierzu auf „Start“ -> „Einstellungen“ -> „Konten“ -> „Familie und andere Benutzer“ (je nach Betriebssystem). Ein Erklärvideo findet sich auch bei Microsoft direkt (z.B. für Windows 10)

3 Videokonferenz-Tools

3.1 Was ist beim Einsatz von Videokonferenz-Tools zu beachten?

Persönlicher Unterricht ist in vielen Fällen nur eingeschränkt oder gar nicht möglich. Daher suchen Eltern und Lehrkräfte nach alternativen Wegen, um den Unterricht durchführen zu können. Geeignet erscheinen Softwareanwendungen, die die Möglichkeit einer Videotelefonie bieten. Dadurch können sich die Beteiligten nicht nur hören, sondern auch sehen und das Gefühl des Miteinanders in der Klasse ist zumindest teilweise vorhanden.

3.2 Auszug von Datenschutzanforderungen

	Wichtige Auswahlkriterien aus Sicht des Datenschutzes			
	Anforderung	**Erläuterung**	**Erfüllt Ja**	**Nein**
1	**Europäischer Speicherort/Anbieter**	Die Speicherung von Daten sollte bevorzugt auf eigenen, selbstgehosteten Systemen oder auf den Endgeräten der Nutzer erfolgen. Europäische Anbieter sind aus Datenschutzsicht in vielen Fällen außereuropäischen vorzuziehen, da Zusatzanforderungen gelten, wenn Daten außerhalb von Europa fließen. Insbesondere wenn sensible oder besondere personenbezogene Daten verarbeitet werden, sind europäische Anbieter vorzuziehen.		
2	**Auftragsverarbeitung** bei Betrieb durch den Dienstleister	Zur Erfüllung gesetzlicher Anforderungen ist der Abschluss eines Datenschutzvertrags (sogenannte Auftragsverarbeitung) mit dem Anbieter erforderlich, wenn das Tool durch den Anbieter betrieben wird.		
3	**Angemessener Schutz der Daten**	Der Anbieter muss angemessene Schutzmaßnahmen zum Schutz der Daten nachweisen können, z.B. durch eine Zertifizierung (ISO 27001, ISO 27018, BSI-Grundschutz).		
4	**Keine / möglichst geringe Datennutzung durch Dienstleister**	Dienstleister dürfen die Daten nur zum Betrieb und zur Gewährleistung des Systems verarbeiten. Je nach Anbieter ist es auch möglich, dass diese Metadaten (wer hat wann mit wem kommuniziert?) oder Inhaltsdaten für eigene Zweck auswerten oder an Dritte weitergeben. Videokonferenz-Tools oder Messenger Apps für die Kommunikation mit Kindern oder Eltern dürfen keine Werbung enthalten.		

	Wichtige Auswahlkriterien aus Sicht des Datenschutzes			
	Anforderung	**Erläuterung**	**Erfüllt Ja**	**Nein**
5	**Sichere Authentifizierung**	Sollen sensible oder besondere personenbezogene Daten ausgetauscht werden, oder erfolgt Kommunikation mit Kindern und Eltern, so ist sicherzustellen, das nur berechtigte Personen Zugang zu dem System erhalten. Es sind hierfür sichere Authentifizierungsmethoden gegenüber der Schule sicherzustellen (z.B. Schule vergibt Login-Daten).		
6	**Verschlüsselung vorhanden**	Der Datenfluss zwischen den Rechnern der Teilnehmer und dem Server des Anbieters muss transportverschlüsselt sein. Noch besser ist es, wenn eine Ende-zu-Ende-Verschlüsselung angeboten wird.		
7	**Löschung von Daten**	Es ist sicherzustellen das Anmelde-, Inhalts- und Nutzungsdaten gelöscht werden können, so dass diese nicht wiederherzustellen sind. Besonders wenn ein Schüler oder Lehrer die Schule verlässt oder die App nicht mehr genutzt wird, sind nicht aufbewahrungspflichtige Daten zu löschen.		
8	**Minimierte Datennutzung des Tools / App**	Die Datenverarbeitung hat so minimal wie möglich zu erfolgen. Daten zur Verwendungsanalyse oder zur Ermittlung des Standortes sind untersagt. Hinweise wann eine Nachricht gelesen wurde, sind in der Regel nicht erforderlich. Erfolgt eine direkte Kommunikation zwischen Eltern, Lehrern und Schülern so ist darauf zu achten, dass Daten von Teilnehmern (Kontaktdaten, Nachrichten im Chat etc.) auf das erforderliche Maß zu reduzieren sind. Ein spezielles Problem bei Messenger Apps ist die Verwendung von Kontaktdaten durch den Anbieter. Hierbei werden alle Kontakte im Kontaktbuch des Nutzers automatisiert an den Anbieter der App gesendet: Dieser nutzt die Daten in der Regel, um feststellen zu können, welcher Kontakt ebenfalls die App verwendet. Problematisch ist, dass dabei auch Daten von Personen betroffen sind, die nicht die App verwenden. Dies ist unzulässig. Ein Upload der Kontaktbücher zum Anbieter darf nicht stattfinden.		

Die Liste stellt einen Auszug wichtiger datenschutzrelevanter Themen dar. Es besteht kein Anspruch auf Vollständigkeit.

Die Videokonferenz-Tools müssen nicht zwingend auf Servern von externen Dienstleistern installiert sein. Bei einigen Tools ist der Betrieb auf Servern der eigenen Schule möglich. Allerdings sind Schulserver oder die Bandbreiten häufig nicht so leistungsfähig, wie die von Dienstleistern, so dass die Verbindungsqualität schlecht werden kann und Verbindungen unterbrochen werden können. Gerade diese Punkte sind für die Beteiligten sehr ärgerlich.

3.3 Worauf beim praktischen Einsatz zu achten ist

Neben diesen allgemeinen Datenschutzanforderungen, die Ihre Datenschutzbeauftragten und IT-ler bewerten müssen, gibt es weitere Herausforderungen beim Einsatz solcher Tools.

Tipp Nr. 1: Nur offizielle Tools verwenden – Bitte verwenden Sie nur die die offiziellen Tools, die Ihnen Ihre Schule empfiehlt!

Tipp Nr. 2: Vertrauliche Kommunikation sicherstellen!

- Verwenden Sie unterschiedliche Passwörter / Einwahlnummern für den Unterricht / die geplante Besprechung.
- Legen Sie immer Passwörter für die geplante Besprechung fest (Anmerkung: Tipps für sichere Passwörter weiter oben beachten!). Verwenden Sie keine feste Systematik, so dass ein Gesprächspartner Einwahlnummer oder Passwort erraten könnte, z.B. durch Hochzählen.
- Veröffentlichen Sie Einwahlnummer und Passwörter nicht online und weisen Sie auch Eltern und Schüler daraufhin, dass sie die Zugangsdaten nicht an Unbefugte weitergeben.
- Teilen Sie den Gesprächspartnern das Passwort über einen separaten Kanal, z.B. per Telefon, SMS oder Messenger etc. mit.
- Nutzen Sie die Option der „Weichzeichnung“ Ihres Bildhintergrundes und weisen Sie die Schülerinnen oder Eltern auf die Nutzung dieser Funktion hin, sofern diese vorhanden ist.
- Verwenden Sie ausschließlich die Video- und Audiofunktionen der Lösung. Verzichten Sie auf die Nutzung des Textchats, da nicht immer festgestellt werden kann, wo die Daten dieser Chats verbleiben. Bei einigen Lösungen gilt die Ende-zu-Ende Verschlüsselung z.B. nicht für den Text-Chat.
- Tauschen Sie keine Dokumente über die Lösung aus (siehe Kapitel Sicherer Datenaustausch)
- Stellen Sie sicher, dass die Videokonferenz vollständig beendet wird. Wenn Sie Moderator sind, verlassen Sie die Videokonferenz als letzter und löschen sie ggf. die Konferenz. Ist dies nicht möglich, vergeben Sie ein neues Passwort.
- Stellen Sie sicher, dass die Teilnehmer der Videokonferenz auch die sind, die Sie vorgeben zu sein. Fordern Sie hierzu u.U. die Teilnehmer auf, ggf. deaktivierte Kameras zu aktivieren. Wenn Sie sicher sind, dass nur die erwünschten Teilnehmer dabei sind, können alle die Kameras wieder deaktivieren. Entfernen Sie unbekannte Teilnehmer aus der Videokonferenz.

Tipp Nr. 3: Aufzeichnungen nur mit Einwilligung oder ganz darauf verzichten!

Aufzeichnungen von Videokonferenzen sind nur mit Einwilligung aller Teilnehmer möglich und nur dann wenn die Aufzeichnung erforderlich ist. Sie müssen alle beteiligten Personen fragen, ob eine Aufzeichnung gestartet werden darf. Wenn dies von allen Personen bejaht wird, so starten Sie die Aufnahme und fragen Ihre Teilnehmer erneut, damit die Einwilligung ebenfalls aufgezeichnet wird. Das erleichtert es erheblich, im Nachgang die Einwilligung nachzuweisen. Bitte speichern Sie die Aufzeichnung an einem sicheren Ort und löschen Sie diese, sobald der Zweck für den die Aufzeichnung erfolgt ist, entfallen ist.

Da für eine gültige Einwilligung von Schülern in der Regel auch die Eltern einwilligen müssen, dürfte der Verzicht auf eine Aufzeichnung in vielen Fällen der bessere Weg sein.

In der schulischen Praxis dürfte in vielen Fällen keine Notwendigkeit einer Aufzeichnung bestehen. Verzichten Sie also immer darauf, wenn es nicht unbedingt erforderlich ist!

3.4 Produktempfehlungen für Schulen

Die folgenden Produktempfehlungen können aus unserer Sicht an Schulen datenschutzkonform eingesetzt werden. Bitte sprechen Sie dennoch immer vorher mit den verantwortlichen Personen an Ihrer Schule! Der Landesdatenschutzbeauftragte in Baden-Württemberg empfiehlt z.B. die folgenden Produkte, die insbesondere von Schulen auf der eigenen Architektur betrieben werden können und kostenlos sind:

- Nextcloud Talk
- BigBlueButton
- Matrix
- RocketChat
- Jitsi Meet

3.5 Produktempfehlungen für einzelne Lehrkräfte

Wenn Sie nicht als Lehrkraft unmittelbar an einer Schule arbeiten, dann werden Sie in vielen Fällen Ihr Videokonferenz-Tool alleine auswählen müssen. Für diesen Fall sprechen wir einzelne Produktempfehlungen aus Sicht des Datenschutzes aus, die von Dienstleistern bereitgestellt werden. Die Auflistung berücksichtigt zusätzlich eine schnelle Einsetzbarkeit und ob die Nutzung kostenlos möglich ist. Sie ist nicht abschließend. Wir stehen in keiner Verbindung zu den Dienstleistern und erhalten keine Vergütung oder sonstige Vorteile.

	Microsoft Teams	GotoMeeting	Blizz

Anbieter - Link zum Produkt	Microsoft Ireland Operations Limited	LogMeIn Ireland Limited	TeamViewer Germany GmbH
Abschluss Auftragsverarbeitung	Im Vertrag integriert	Datenverarbeitungsnachtrag	Abschluss mit Zustimmung zur EULA
Angemessenes Datenschutzniveau	Im Vertrag integriert mit EU-Standard-Vertragsklauseln	Im Vertrag integriert mit EU-Standard-Vertragsklauseln bzw. Privacy Shield	Europäischer Anbieter
Hosting in dt. Rechen-zentrum möglich	für Bezahlvariante	unbekannt	Laut Subunternehmer-liste Deutschland /Österreich
Bewertung der Daten-schutzkonformität	einsetzbar	einsetzbar	einsetzbar
Kostenlos für Schulen und Lehrkräfte?	Aktuell kostenlos	Für 14 Tage kostenlos	kostenlos für Schulen und Universitäten bis 31.07.2020

Stand Anfang Juli 2020 hat sich gegenüber der Erstveröffentlichung unseres White Papers bei Videokonferenztools so manches getan. Am 03. Juli hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) unterschiedliche Arbeitsergebnisse veröffentlicht. Unter anderem sind das Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, Empfehlungen für die Prüfung von Auftragsverarbeitungsverträgen von Anbietern von Videokonferenzdiensten, Empfehlungen zur Durchführung von Videokonferenzen und eine Checkliste für die Durchführung von Videokonferenzen.

Die veröffentlichten Stellungnahmen sind ernüchternd. Unsere oben auf dieser Seite genannten Empfehlungen werden als nicht einsetzbar bewertet, da es Mängel in der Vereinbarung zur Auftragsverarbeitung gäbe. Schaut man sich im Detail die sonstigen geprüften Tools an, so fällt auf, dass kein einziges als einsetzbar bewertet wird, da es entweder juristische oder technische Mängel gäbe. Die Stellungnahmen aus Berlin sind Gegenstand hitziger Diskussionen und es gibt gerade von Datenschutzbeauftragten heftige Kritik an der Bewertung des BlnBDI. Ob die Aussage und Bewertung, dass kein einziger Dienst datenschutzkonform sein soll Realitätsbezug zur aktuellen Situation hat, muss jeder für sich selbst entscheiden.

Die kostenlose Version von Microsoft Teams hat ebenfalls einen Haken. Nach aktueller Kenntnislage ist für die kostenlose Version derzeit der Abschluss der Auftragsverarbeitung nicht möglich. Das wiederum wäre wieder ein Ausschlusskriterium. Wir warten auf die Antwort des Datenschutzbeauftragten von Microsoft dem wir diesen Missstand mitgeteilt haben.

3.6 Ist Zoom einsetzbar?

Die eine oder andere Lehrkraft wundert sich bestimmt, weshalb wir keine Empfehlung für Zoom aussprechen. Wer die Berichtserstattung der letzten Monate nicht mitverfolgt hat, es gibt zwei Lager: Die einen halten Zoom für einsetzbar und datenschutzkonform und freuen sich, wie schnell Zoom bekanntgewordene Sicherheitslücken schließt. Außerdem sehen sie Zoom als Opfer ausufernder Kritik.

Denn das ist die Position des anderen Lagers. Diese Gruppe steht Zoom sehr kritisch gegenüber, da Zoom mit so ziemlich jedem Datenschutz- und IT-Sicherheits-Fettnäpfchen in Verbindung gebracht wurde (z.B. Zoom-Bombing, Datenfluss an Facebook, Datennutzung für eigene Zwecke, mangelnde Verschlüsselung). Entscheiden Sie selbst.

Am 24. Juni berichtete Stefan Brink, der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg von Fortschritten bei Zoom. In der aktuellen Version Zoom 5.0 gibt es Verbesserungen bei nutzer- und datenschutzfreundlichen Voreinstellungen, eine wirtschaftliche Datennutzung der User von Zoom ist nun ausgeschlossen und die Bezahlvariante soll Ende-zu-Ende verschlüsselt sein. Letzteres verstehen wir nicht. Sicherheit sollte für alle Nutzer gleichermaßen verfügbar sein und nicht nur für Bezahlkunden.

4 Messenger Apps

4.1 Wie können Messenger Apps Lehrkräfte unterstützen?

Messenger App ist nicht gleich Messenger App. Mittlerweile gibt es eine Vielzahl von Funktionen, die in den Apps existieren, die je nach Anbieter anders ausgestaltet werden. Um eine geeignete App auswählen zu können, sollte daher klar sein, welche Funktionen für die Arbeit im Schulbetrieb erforderlich sind.

	Wichtige Funktionen und Fragen bei der Auswahl				
	Funktion	Erläuterung	Erforderlich: Ja	Nein	Nicht erwünscht
1	**Gruppenchat**	Kommunikation mit mehreren Teilnehmern gleichzeitig (alle können Nachricht lesen und schreiben)			
2	**Broadcast**	Eine Person kann an eine Liste von Empfängern Nachrichten versenden, ohne dass die Empfänger sich untereinander kennen, sehen oder austauschen können. Je nach Form können die Empfänger ggf. nicht antworten.			
3	**Linkfreigabe**	Jeder mit einem Link kann einer Gruppe oder einem Broadcast beitreten und muss nicht vom Versender persönlich aufgenommen werden.			
4	**Bildnachrichten**	Bilder können als Nachricht versendet werden. Welche können das sein?: • Aufgenommene mit dem Smartphone / PC -Kamera • Aus der Galerie des Smartphones • Vorgefertigte GIFs / Glyphicons / Smileys aus der Programmbibliothek			
5	**Sprachnachrichten**	Aufnehmen von Audiosignalen (meist über das Mikro), die als Nachricht versendet werden und wiederholt angehört werden können.			
6	**Videonachrichten**	Aufnehmen von Video- und Audiosignalen (meist über das Mikro und die Kamera), die als Nachricht versendet werden und wiederholt angesehen werden können.			
7	**Kontakte senden**	Kontakte im Kontaktbuch können über die App versendet werden, so dass diese beim Empfänger direkt ins Kontaktbuch übernommen werden können.			
8	**VoIP/Anruffunktion**	Telefonanrufe über die Messenger App			

	Wichtige Funktionen und Fragen bei der Auswahl				
	Funktion	Erläuterung	Erforderlich		
			Ja	Nein	Nicht erwünscht
9	**Videotelefonie**	Anrufe über die Messenger App, die zugleich live ein Bild der Kamera aus dem Smartphone/dem PC überträgt.			
10	**Upload**	Hochladen von Dateien (Bildern, Worddokumenten, PDFs, etc.) zum Bereitstellen über die App.			

Bezeichnungen der Funktionen können je nach Messenger abweichen, zudem geht die Liste auf wichtige datenschutzrelevante Themen ein. Es besteht kein Anspruch auf Vollständigkeit.

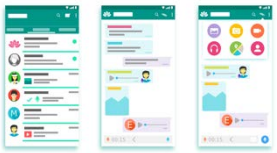
Weitere Aspekte können sein:

- **Freie Kommunikation der Clients -** Der Großteil der Messenger Apps ist auf eine freie Kommunikation ausgerichtet, das heißt, dass jeder mit jedem Kommunizieren kann.
- **Verwaltete Kommunikation der Clients -** Die verwaltete Kommunikation ist der Gegensatz zur freien Kommunikation. Administratoren/Verantwortliche legen fest, wer wie mit wem kommunizieren darf (z.B. nur die Klasse als Gruppe, nur Schüler mit dem Lehrer aber nicht untereinander).
- **Asynchrone Kommunikation -** Nachrichten können versendet werden, auch wenn der Empfänger offline ist. Die Nachrichten werden erst zugestellt, wenn der Empfänger wieder online geht.
- **Archivierung -** Speicherung der versandten Nachrichten auf dem Server, auch wenn diese auf dem Smartphone/PC gelöscht wurden.
- **Automatische Löschung -** Versender können für Inhalte festlegen, wie lange diese beim Empfänger sichtbar bleiben und werden nach Ablauf der Zeit automatisch gelöscht.
- **Standort teilen -** Nachricht, die über eine Karte anzeigt, an welchem Standort man sich zum Zeitpunkt des Versendens einer Nachricht befindet.
- **Livestandort -** Der Standort des Teilnehmers wird (meist ab Einschalten der Funktion bis zum Ausschalten) an den Empfänger übertragen, so dass der Empfänger jederzeit sehen kann, wo sich die Person/das Gerät aktuell befindet.
- **Status -** Personen können über den Status aktuelle Informationen zu ihrer Erreichbarkeit oder ihren Aktivitäten teilen. Diese sind nur für einen begrenzten Zeitraum, aber für alle Kontakte sichtbar.
- **Nutzerverifikation auf dem Server –** Nur wer eine Berechtigung erhalten hat, darf die Messenger App nutzen. Dies kann durch vorgegebene Registrierungsverfahren, z.B. Vergabe von Username und Passwort, E-Mail-Registrierung etc. erfolgen.
- **Nutzerverifikation zwischen den Versendern –** Das Problem bei digitaler Kommunikation ist: Wie können User darauf vertrauen, dass sie wirklich mit der richtigen Person kommunizieren? Durch Austausch eines persönlichen Codes (z.B. Scannen eines persönlich QR-Codes) können Personen im realen Leben verifizieren, dass sie mit der Person kommunizieren, mit der sie es vermuten.
- **Speicherung auf dem Endgerät –** Nachrichten werden auf dem verwendeten Gerät gespeichert. Auch ohne Internetempfang können erhaltene Nachrichten/Inhalte eingesehen werden.

4.2 Was ist beim Einsatz von Messenger Apps zu beachten?

Wenn Sie eine Messenger App einsetzen möchten, so müssen Sie einige Datenschutzfragen berücksichtigen. Neben den Anforderungen sollten vorab folgende Fragen geklärt werden:

1. **Wer soll über das System kommunizieren?**



Die rechtliche Bewertung unterscheidet sich je nach Teilnehmerkreis erheblich. Kommunizieren nur Lehrende untereinander? Kommunizieren Lehrerinnen mit Eltern/dem Vormund oder direkt mit Schülern?

2. **Welche Informationen sollen über die Messenger App verarbeitet werden?**

Der Schutzbedarf personenbezogener Daten ist abhängig von den verarbeiteten Daten. Diese können unterschiedlich sensibel sein und je nach Sachverhalt Gefahren für den Betroffenen nach sich ziehen, wenn sie falsch verarbeitet werden. Beispielsweise macht es einen großen Unterschied, ob nur Termine abzustimmen, Erinnerungen anzulegen, Aufgaben zu verteilen oder ob auch sensible oder besondere personenbezogene Daten wie Noten, Krankmeldungen übermittelt oder vertrauliche Kommunikationen bspw. mit dem Vertrauenslehrer stadtfinden soll. Bitte beachten Sie die Auswahlkriterien unter Kapitel 3.2!

Weiterer Aspekt bei der Auswahl ist auch die **Rechtmäßigkei**t. Stellen Sie sicher, dass Sie personenbezogene Daten nur rechtmäßig verarbeiten. Hinterfragen Sie, ob Schüler zur Nutzung der App verpflichtet werden können oder ob dies ein freiwilliges Angebot ist. Werden Standortdaten erhoben, Bilder oder Videos geteilt, wird regelmäßig die Einwilligung der Betroffenen nötig sein. Aufgrund der Fürsorgepflicht der Lehrer und der Schule ist die Verarbeitung von Standortdaten eher abzulehnen.

Auf Messenger Apps treffen wie in anderen digitale Medien unterschiedlichste Meinungen, Interessen und Kulturen aufeinander. Kommunizieren Lehrerinnen mit Schülern und Eltern gemeinsam, sollten deshalb klare **Verhaltensregeln** aufgestellt werden, z.B.:

- Umgang mit Uploads um rechtswidrige und unerwünschte Inhalte zu vermeiden und File-Sharing zu unterbinden.
- Kommunikationsformen und Aufsichten um bspw. Mobbing zu verhindern.
- Umgang mit Videonachrichten und Bildern um Urheberrechts- und Persönlichkeitsverletzungen, auch von Dritten, zu verhindern.
- Erreichbarkeit/Verwendung außerhalb der Schulzeiten (Lehrer haben ebenfalls ein Recht auf Erholung nach Dienstende - ebenso sollten Schüler auch ein Wochenende haben).

4.3 Welche Messenger können wir empfehlen und warum?

Die folgenden Produktempfehlungen können aus unserer Sicht an Schulen weitestgehend datenschutzkonform eingesetzt werden (je nach Daten und Teilnehmern). Bitte sprechen Sie immer vorher mit den verantwortlichen Personen an Ihrer Schule!

- Threema Work
- matrix
- Schul Info-App
- Teamwire
- Schul.cloud

Eine kostenlose Threema Work Lizenz kann für Lehrerinnen an öffentlichen Schulen beim Kultusministerium in Baden-Württemberg bezogen werden.

4.4 Warum kein WhatsApp?

WhatsApp hat seinen Sitz in den USA. Mit Installation der App werden alle Kontaktdaten des Adressbuches in die USA geladen, um dort ausgewertet zu werden. Egal ob der Kontakt im Kontaktbuch WhatsApp nutzt oder nicht. Dies ist unzulässig. Zudem können nach dem US-Patriot-Act Sicherheitsbehörden ohne Wissen der Betroffenen Zugriff auf die Daten nehmen. Dies entspricht nicht dem europäischen Datenschutzverständnis.

4.5 Sind Messenger wirklich erlaubt?

Ein häufiges Argument gegen den Einsatz von Messenger Apps ist das Verbot zur Nutzung von sozialen Netzwerken durch das Ministerium für Kultus, Jugend und Sport in Baden-Württemberg.
Eine Betrachtung des Verbotes zeigt jedoch, dass es dabei um soziale Netzwerke wie Facebook, Google+ oder Twitter geht. Zudem zeigt die Begründung, dass das Verbot besteht, da:

- diese Plattformen keinen ausreichenden Schutz der Persönlichkeitsrechte sicherstellen,
- die Plattformen sich weitreichende Nutzungsrechte der Informationen einräumen und
- die Neutralität der Schulen in Bezug auf Werbung nicht gewährleistet werden kann.

Werden Messenger Apps gesetzeskonform eingesetzt, ist ein Verstoß gegen das ausgesprochene Verbot zur Nutzung von sozialen Medien nicht zu erkennen.

5 Sicherer Datenaustausch zwischen Lehrern und Schülern

Früher oder später kommen Sie in die Situation, dass Sie Daten mit Schülern austauschen müssen. Zum einen sollen die Schülerinnen einfach und unkompliziert Zugang zu Arbeitsblättern und Aufgaben erhalten. Zum anderen müssen die bearbeiteten Arbeitsergebnisse, Hausarbeiten und andere Dokumente wieder an die Lehrer zurückgesendet werden. Unter Umständen können hier auch besonders sensible Daten anfallen, z.B. im Kontext der Gemeinschaftskunde, wenn politische Inhalte und Meinungen geäußert werden oder im Religionsunterricht. Gemäß der Datenschutz-Grundverordnung (DS-GVO) sind diese Arten von Daten besonders schützenswert und es müssen entsprechende technische und organisatorische Maßnahmen für die Sicherheit der Daten getroffen werden.

Im Folgenden betrachten wir einige Möglichkeiten zum Datenaustausch und Probleme, die in dem Zusammenhang auftreten können.

5.1 Datenaustausch via E-Mail

Heutzutage ist es in aller Regel so, dass E-Mails auf dem Transportkanal standardmäßig verschlüsselt werden. An der Kommunikation nicht beteiligte Dritte können die versandten E-Mails nicht ohne weiteres mitlesen. Jedoch können selbst im Falle einer bestehenden Transportkanalverschlüsselung Dritte Kenntnisse von den Inhalten Ihrer Kommunikation erlangen. In der Regel werden sowohl auf Ihrem E-Mail Server, als auch auf dem Server des Empfängers die Nachrichten gespeichert. Somit haben sowohl Administratoren der Server, als auch Hacker, die den E-Mail Server erfolgreich angegriffen haben, potenziell Zugriff auf die dort gespeicherten E-Mails und deren Anhänge.

Überall dort, wo besonders sensible Daten versendet werden sollen, reicht die reine Transportkanalverschlüsselung als Schutz nicht mehr aus und es sind weitreichendere Maßnahmen zu treffen:

5.1.1 Ende-zu-Ende E-Mail Verschlüsselung

Im Gegensatz zu einer Transportkanalverschlüsselung wird bei einer Ende-zu-Ende Verschlüsselung die zu versendende E-Mail beim Versender verschlüsselt und erst wieder beim Empfänger entschlüsselt. Es wird also nicht (nur) der Transportkanal als solches geschützt, sondern die Nachricht selbst. Sowohl auf dem Transportweg, als auch auf den beteiligten E-Mail Servern ist somit eine Kenntnisnahme durch Dritte ausgeschlossen.

Die Einrichtung einer Ende-zu-Ende Verschlüsselung wird in den meisten Fällen jedoch an den Möglichkeiten der Schüler scheitern. Eine Anleitung finden Sie hier auf dem Portal Lehrerinnenfortbildung Baden-Württemberg.

5.1.2 Passwortgeschützte Dateianhänge

Zur Absicherung von sensiblen Inhalten können Dateianhänge mit einem Passwortschutz versehen werden. Hierfür gibt es eine Vielzahl an kostenlosen Anwendungen (z.B. 7-ZIP), die es den Anwendern ohne besondere IT-Kenntnisse ermöglichen, einzelne Dateien / mehrere Dateien oder Dokumente zu

einem Archiv zusammenzufügen. Das Archiv wird seitens der Anwendung automatisch erstellt und mit sicheren Verschlüsselungsalgorithmen abgesichert. Einzelne Office Dokumente können in neueren Office Versionen mit wenigen Mausklicks passwortgeschützt werden: Datei -> Informationen -> Dokument schützen -> „mit Kennwort verschlüsseln“. Eine Anleitung zum Entpacken von Dateien mit dem Programm 7-ZIP finden Sie hier.

Beiden Verfahren gemein ist, dass der Anwender ein hinreichend sicheres Passwort (siehe Empfehlungen im Kapitel 2.1.1) wählen sollte. Der Passwortaustausch sollte unbedingt auf einem anderen Kommunikationsweg (Telefon, SMS, Messenger, FAX, schriftlich, etc.) erfolgen.

5.2 Sonstige Hinweise im Umgang mit E-Mails

5.2.1 Carbon Copy vs. Blind Carbon Copy

E-Mail Anwendungen bieten Ihnen die Möglichkeit der so genannten Carbon Copy ("Cc…"-Versand). Beim "Cc…"-Versand können alle Empfänger die Adressen der restlichen Empfänger einsehen. Zum einen ist dies problematisch, weil die Schüler untereinander unter Umständen nicht ihre E-Mail-Adressen teilen wollen. Zum anderen kann dies aus Datenschutzsicht zu einer Datenpanne führen. Daher empfehlen wir Ihnen für die Kommunikation mit mehreren Schülern grundsätzlich die „Blind Carbon Copy“ ("Bcc…"). Sie können ebenso wie bei der "Cc…"-Funktion mehrere Empfänger zeitgleich kontaktieren. Diese haben aber keine Kenntnis von den Adressen der anderen Empfänger. Dies verhindert es auch, dass ein Schüler versehentlich allen antwortet und somit seine Arbeitsergebnisse in der Klasse verteilt.

5.2.2 Verwendung privater E-Mail Accounts

Neben dem "Bcc…"-Versand von E-Mails ist sicherzustellen, dass Sie als Lehrer keine privaten E-Mail-Adressen für die Kommunikation verwenden. Die Schule ist im Sinne des Datenschutzes verantwortliche Stelle und in der Pflicht die Sicherheit der Datenverarbeitung zu gewährleisten. Diese Kontrolle erfolgt bei den von der Schule eingesetzten IT-Systemen und wird durch Datenschutzbeauftragte begleitet. Sofern keine eigenen E-Mail Server betrieben werden, sondern dritte Provider, sind datenschutzrechtliche Verträge zu schließen, um die Rechtmäßigkeit der Datenweitergabe herzustellen. Diese Möglichkeit besteht bei privaten E-Mail-Adressen in der Regel nicht und ist durch die verantwortliche Stelle (der Schule) nicht zu tolerieren. Sehen Sie daher von der Nutzung privater E-Mail Accounts besser ab.

5.2.3 E-Mail Archivierung

Ein weiteres Problem bei der Verwendung von E-Mails als Möglichkeit zum Datenaustausch ist unter Umständen ein E-Mail Archiv, welches von der Schule eingerichtet wurde. Gemäß der DS-GVO sind Daten nach Zweckentfall (und unter Berücksichtigung der Aufbewahrungsfristen) zu löschen. Bei aktivem E-Mail Archiv werden sämtliche E-Mails jedoch bis zu 10 Jahre gespeichert. Somit wird unter Umständen direkt gegen Grundsätze (Speicherbegrenzung) des Datenschutzrechtes verstoßen. Es ist daher vor Datenaustausch via E-Mail zu prüfen inwiefern ein E-Mail Archiv verwendet wird.

5.3 Fazit Datenaustausch via E-Mail

Grundsätzlich spricht nichts gegen den Austausch von Daten via E-Mail, sofern folgende Aspekte berücksichtigt werden:

- Keine Verwendung privater E-Mail Accounts (Lehrer)
- Nutzung der "Bcc…"-Funktion
- Schutz sensibler Inhalte mit passwortgeschützten Dateien oder Archiven
- Klärung der E-Mail Archivierung mit der IT-Abteilung und dem Datenschutzbeauftragten

Neben der Verwendung von E-Mail gibt es noch weitere, zum Teil deutlich komfortablere Lösungen, um Daten auszutauschen.

5.4 Datenaustausch via Cloud

Der Begriff Cloud ist nach wie vor in aller Munde, daher an dieser Stelle nur eine kurze Erklärung: Cloud-Speicher ermöglichen es, Dateien und Dokumente auf einem entfernten Server zu speichern und via Internet jederzeit darauf zuzugreifen. Mit entsprechenden Berechtigungskonzepten können Dateien mit anderen Nutzern geteilt und ausgetauscht werden. Dies geht in aller Regel auch mittels Web-Browser. Neben der Möglichkeit zur Anlage von Nutzern, bei dem jeder Schüler einen eigenen Account erhält und Dateien abrufen und ablegen kann, besteht bei vielen Cloudlösungen auch die Möglichkeit zu so genannten Freigabe-Links. Dies kann wie folgt aussehen:

Sie als Lehrer können mit Ihrem Account einen Ordner anlegen und diesen via Link freigeben. Alle Empfänger dieses Links können die dort abgelegten Dateien via Browser abrufen und herunterladen. Ein solcher Ordner bietet sich an, sofern Aufgabenblätter verteilt werden sollen. Auch Freigabe-Links können mit Passwörtern vor unbefugtem Zugriff geschützt werden. Für den Weg vom Schüler zum Lehrer kann ebenfalls eine entsprechende Konfiguration gewählt werden: Sie als Lehrer erstellen einen Ordner, für den die zugreifenden Schüler ausschließlich Schreibzugriff haben. Die Schüler können Dateien in diesen Ordner hochladen, sie können jedoch keine darin befindlichen Dateien abrufen.
Sofern Ihre Schule bereits eine eigene Cloud betreibt oder einen Dienstleister verwendet, ist die oben beschriebene Möglichkeit einfach und unkompliziert einzurichten.

Sofern seitens der Schule noch keine Cloud eingerichtet wurde, beachten Sie die Kriterien im Kapitel 3.2. Auszug von Datenschutzanforderungen!

5.4.1 Fazit Datenaustausch via Cloud

Der Datenaustauch via Cloud stellt eine einfache und zuverlässige Möglichkeit zum Datenaustausch dar. Voraussetzung für die Nutzung ist eine korrekte Einrichtung durch die IT, die unter Umständen viel Zeit und Ressourcen verschlingt. Beim Betrieb und der Nutzung durch die Anwender rentiert sich der vorgelagerte Aufwand jedoch in den meisten Fällen. Bei korrekter Konfiguration müssen die Anwender nur noch wenige Hinweise beachten.

Ob eine Cloud datenschutzkonform einsetzbar ist, hängt von vielen Faktoren ab und ist zwingend mit Ihrem Datenschutzbeauftragten zu klären. Die Nutzung von privaten Clouds wie z.B. Dropbox ist unzulässig!

5.5 Datenaustausch via Datenträger

Wenn Sie weder verschlüsselte E-Mails, verschlüsselte Dateianhänge oder eine datenschutzkonforme Cloud nutzen können, so besteht noch die Möglichkeit zum Austausch via USB-Stick, CD oder externer Festplatte. Der Verlust eines solchen Datenträgers könnte jedoch je nach Umstand eine Datenpanne darstellen. Insbesondere wenn Sie als Lehrer den USB-Stick verlieren, auf dem Arbeitsergebnisse mit personenbezogenen Daten von Schülern waren. Zur Absicherung von externen Datenträgern können diese über Windows Bordmittel verschlüsselt werden. Die Verschlüsselung stellt im Falle eines Verlustes sicher, dass Dritte keinen Zugriff auf die Daten nehmen können. Zum Öffnen des Datenträgers ist ein Passwort zu vergeben. Neben dem Schutz des Datenträgers vor unbefugten Zugriffen ist vor Verwendung der Inhalte ein Suchlauf mit einer Anti-Viren-Software durchzuführen.

Sofern Ihre Schule Ihnen die Verwendung privater USB-Sticks erlaubt, sind dennoch die vorgenannten Sicherheitsmaßnahmen zu beachten (siehe auch Punkt 2.1.1)

Verwenden Sie keine privaten Wechseldatenträger für den Datenaustausch. Für einen solchen Fall sollte die Schule entsprechende Datenträger anschaffen und zur Verfügung zu stellen.

6 Auswahl einer geeigneten Schul-/Lernplattform

Vor Corona wurde das große Potential der Digitalisierung im Bereich von Schulen größtenteils noch nicht ausgeschöpft. Bedingt durch die neue Situation und der Beachtung der Vorgaben der Corona-Verordnung(en) ergibt sich daher in dieser Krise die Chance den Entwicklungsstau an dieser Stelle aufzulösen und die Geschwindigkeit zur Digitalisierung zu beschleunigen.

In der Auseinandersetzung mit diesem Thema stellen sich den Lehrkräften während des Lockdowns/Shutdowns und auch nach (begrenzter) Wiederaufnahme des Schulbetriebs oftmals folgende Fragen:

- Wie können wir uns während der Coronakrise organisieren?
- Welche Online-Plattformen oder andere digitale Hilfsmittel erleichtern uns Lehrkräften den Austausch mit den Schülerinnen und Schülern?
- Wie berücksichtige ich die unterschiedliche Ausstattung (Hardware, IT-Infrastruktur zuhause) der Schülerinnen
- Welche Lerninhalte sind derzeit überhaupt geeignet und in digitaler Form vorhanden/vermittelbar?

Bei all diesen Fragen ist die Auswahl einer für den individuellen Schulbetrieb geeigneten Schul-/Lernplattform (oder auch Lernmanagement-Software) entscheidend. Das Angebot ist vielfältig und jede Lösung bietet unterschiedliche Eigenschaften. Sie interessiert vor allem, welche Lösungen die Plattform zur Unterrichtsgestaltung mitbringt und ob Methodik und Didaktik bei der Wissensvermittlung in gleicher Weise umsetzbar ist wie im Präsenzunterricht. Ihre Schulleitung hat ergänzend dazu auch Überlegungen zur Finanzierbarkeit anzustellen und Ihre interne IT wiederum schaut auf Datensicherheit. Die Datenschützer wollen gewährleistet wissen, dass das Persönlichkeitsrecht der Beteiligten/Betroffenen gewahrt ist.

In Baden-Württemberg hat sich die Ministerin für Kultus, Jugend und Sport, Frau Dr. Susanne Eisenmann, in enger Abstimmung mit den Fachleuten des Landeshochschulnetzes BW für "*Moodle*" stark gemacht. Es ist das weitverbreitetste Tool und für Schulen in BW wird eine kostenfreie Nutzung angeboten. In recht kurzer Zeit sind dabei 4.000 neue "*Moodle*"-Schulaccounts entstanden. Die Nutzungsfrequenz ist enorm und lag bereits Ende März 2020 bei knapp 20 Millionen Aufrufen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) fordert explizit alle Schulen und Lehrkräfte auf, diese "*vom Land kostenlos zur Verfügung gestellte datenschutzfreundliche Lernplattform mitsamt des besonders auf das Online-Lernen zugeschnittenen Videokonferenzsystems BigBlueButton zu nutzen*", da praxisgerecht und datenschutzkonform (Pressemitteilung vom 29. April 2020). Da die Lernplattform durch eine eigene Stelle des Landes betrieben wird (Belwue), ist gewährleistet, dass kein Datenabfluss an Dritte erfolgt. In der Konfiguration des Belwue ist Moodle datenschutzrechtlich geprüft und zulässig. Auf der Homepage der Fortbildung für Lehrerinnen finden Sie unter dem Menüpunkt E-Learning umfangreiche Informationen zu "*Moodle*".

Da sich die meisten Schulen bereits für den Einsatz von "*Moodle*" entschieden haben, haben auch wir dieses Tool in den Fokus unserer Betrachtung gestellt. Selbstverständlich gibt es auch weitere Anbieter

und deren Softwarelösungen. So zum Beispiel die "*HPI Schul-Cloud*", die vom Hasso-Plattner-Institut und dem Verein MINT-EC entwickelt wurde. Daher ist diese Aufzählung nicht abschließend und „*Moodle*“ beispielhaft (insbesondere durch die Empfehlung des LfDI BW) genannt.

Alle Tools wollen jedoch gewährleisten, dass darin die gemeinsamen Aufgaben in der Zusammenarbeit zwischen Lehrkräften, Schülern und Erziehungsberechtigten abgebildet sind: digitales Lernen, Unterrichten und Kommunizieren.

Dabei sollten, wenn möglich die nachfolgenden Anforderungen innerhalb der Tools ermöglich sein.

Wünschenswerte Ausstattung von Lernplattformen		
Anforderung	Erfüllt	
	Ja	Nein
Mit Schülerinnen und Schülern chatten, sie per Videokonferenz unterrichten und dabei Dokumente oder die eigene Desktopansicht teilen (**Kommunikation**).		
Gemeinsam Ideen sammeln, Texte verfassen, Projekte planen oder Grafiken zeichnen, digitale Pinnwände, Schreibflächen und Tafeln sollen gemeinsames Arbeiten am Computer, Tablet oder Smartphone ermöglichen. Lerngruppen einrichten, Aufgaben und Materialien an die Schülerinnen und Schüler ausgeben sowie deren Arbeiten entgegennehmen und bewerten (**Kollaboration**).		
Eigene interaktive, multimediale Lernbausteine für Ihre Schüler/-innen erstellen: von Multiple-Choice-Fragen über Zuordnungsaufgaben bis hin zu Videos mit Einblendungen (**Interaktive Aufgaben**).		
Mit einfachen Mitteln ein Erklärvideo für Ihre Schüler/-innen erstellen (**Erklärvideos**).		
Programmieren, Graphen darstellen oder Diagramme analysieren. Fachunterricht digital gestalten können (**Fachunterricht**).		

Alle Punkte in Gesamtheit werden innerhalb eines Tools wohl nicht angeboten werden, so dass die Lernplattform durch weitere geeignete Lösungen ergänzt werden kann.

Das Landesmedienzentrum Baden-Württemberg hat dazu eine Übersicht geeigneter Tools für die unterschiedlichen Nutzungen bzw. Ausrichtungen zusammengestellt.

Wir können und wollen an dieser Stelle keine Empfehlung abgeben, da aus den o.g. Gründen/Aspekten die eine oder andere Lösung für die Entscheidungsträger als besser geeignet erscheint. Was wir Ihnen durch unsere Expertise gerne anbieten ist, ob bei der Auswahl der Tools Datenschutzanforderungen ausreichend berücksichtigt sind. Bitte berücksichtigen Sie daher zunächst, dass nicht alle dieser Tools auf datenschutzkonforme Nutzbarkeit überprüft wurden und bei Bedarf diese Überprüfung noch stattfinden muss.

Vielleicht ist gerade jetzt die Zeit sich mit dem Schritt aus der analogen zur digitalen Welt auseinanderzusetzen. Im Bereich e-Learning erhalten Sie eine große Auswahl an interessanten Lerninhalten, die Ihre eigenen Angebote oder Materialen in Papierform mittelfristig ergänzen oder ganz ersetzen könnten.

Auf der Homepage des deutschen Bildungsservers stellt Ihnen das DIPF | Leibniz-Institut für Bildungsforschung und Bildungsinformation eine umfangreiche Auswahl an Unterrichtsmaterialien zur Verfügung, die größtenteils unentgeltlich bezogen werden können.

7 Hilfreiche Links zu weiterführenden Informationen

- Medienwerkstatt: Sicherheit am Rechner auf dem Portal Lehrerinnenfortbildung Baden-Württemberg
- Hinweise der Aufsichtsbehörde Baden-Württemberg zu datenschutzfreundlichen Möglichkeiten der Kommunikation, vom 17. April 2020
- Hinweise der Aufsichtsbehörde Baden-Württemberg zu "Unterstützung von Schulen", vom 19. März 2020
- Hinweise des Kultusministeriums BW zu Lern- und Kommunikationsplattformen
- Schreiben des Kultusministeriums BW vom 16.03.2020 zur kostenlosen Nutzung und sofortigen Verfügbarkeit von "Moodle"
- Messenger für Lehrkräfte, kostenlose Threema Work Lizenz beim Kultusministerium BW.
- Pressemitteilung des LfDI Baden-Württemberg zu Threema an Schulen, vom 29. April
- Kurzprüfung von Videokonferenzdiensten – BlnBDI veröffentlicht Ergebnisse, vom 03. Juli
- Warnung des LFDI wurde gehört – Zoom bessert nach, vom 24. Juni

Karlsruhe und Stuttgart, den 10.07.2020

Erstellt von der ENSECUR GmbH in gemeinsamer Ausarbeitung von Steven Bösel, Julian Häcker, Thorsten Jordan, Michael Konitzer und Bastian Maute.

Über die Autoren
ENSECUR ist ein Beratungsunternehmen für Datenschutz und Datensicherheit. Wir unterstützen als Datenschutzbeauftragte kleine und mittelständische Unternehmen in Baden-Württemberg, insbesondere:

- Softwareunternehmen mit Datenschutzanforderungen von Auftraggebern
- Soziale Einrichtungen mit gesetzlichen und kirchlichen Datenschutzanforderungen
- Industrieunternehmen mit gesetzlichen Datenschutzanforderungen

Mission
Wir brennen für Datenschutz und wollen diese Begeisterung an Sie und Ihre Organisation weitergeben, um gemeinsam mit Ihnen Ihre Datenschutzziele zu erreichen.

Bildquellen:

S.15 oben: Bild von 200degrees auf pixabay
S.15 unten: Bild von TheDigitalArtist auf pixabay

Bitte beachten Sie, dass dieses Whitepaper trotz großer Sorgfalt keinen Anspruch auf Vollständigkeit hat und natürlich auch keine rechtliche Empfehlung bedeuten soll. Aufgrund der hohen Dynamik sind alle Angaben ohne Gewähr.