Leitfaden für die datenschutzkonforme Auswahl und den Betrieb von Lern-, Informations- und Kommunikationsplattformen an Schulen

Die Auswahl und der spätere Betrieb von Lern-, Informations- und Kommunikationsplattformen gehen mit der Beurteilung komplexer datenschutzrechtlicher Fragestellungen einher. Die vorliegende Handreichung soll Schulen und anderen Stellen dabei unterstützen, eine datenschutzkonforme Plattform zu *identifizieren* bzw. auszuwählen und einen *Betrieb* entsprechend den gesetzlichen Vorgaben zu gewährleisten.

Lern-, Informations- und Kommunikationsplattformen können von Schulen aus didaktisch- pädagogischen Gründen genutzt werden. Der Einsatz wird durch § 1 SchG (Erziehungs- und Bildungsauftrag) abgedeckt. Die verarbeiteten Daten dürfen nur für diese Zwecke genutzt werden, eine darüber hinausgehende Verarbeitung ist unzulässig.

Allerdings wird an dieser Stelle darauf hingewiesen, dass datenschutzrechtliches und informationstechnisches Grundwissen vorhanden sein muss, um diese Auswahl sachgerecht treffen zu können. Aufgrund der Komplexität der Materie kann das vorliegende Dokument daher nur als Hilfestellung dienen.

Generell gilt, dass die jeweilige Schule immer die datenschutzrechtlich verantwortliche Stelle bei der Nutzung der Plattformen bleibt - auch dann, wenn die Plattform durch einen Dienstleister zur Verfügung gestellt wird. Das bedeutet, dass die Schule die Rechtmäßigkeit der Datenverarbeitung sicherstellen muss. Die Rechtmäßigkeit bezieht sich insbesondere auf Art und Umfang der Datenverarbeitung, also darauf welche Datenarten auf welche Weise verarbeitet werden. Darüber hinaus ist auch auf die Art und Weise und den Zweck eventueller Übermittlungen zu achten, erfolgt z.B. eine Datenübermittlung zu Werbezwecken, wie es bei vielen solcher Plattformen der Fall ist (was beim Einsatz an Schulen unzulässig ist). Die Schule muss auch sicherzustellen, dass technische und organisatorische Datenschutzmaßnahmen nach Art. 32 Abs.1 EU-DSGVO getroffen werden, z.B. die Verhinderung unbefugten Zugriffs.
Ferner ist die Schule dafür verantwortlich, folgende Rechte der Betroffenen zu wahren:

- Auskunftsrecht (Art. 15 EU-DSGVO)
- Recht auf Berichtigung (Art. 16 EU-DSGVO)
- Recht auf Löschung (Art. 17 EU-DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 EU-DSGVO)
- Datenübertragbarkeit (Art. 20 EU-DSGVO)
- Widerspruchsrecht (Art. 21 EU-DSGVO)

Das bedeutet, dass die Schule in all diesen Fällen die Betroffen bzw. auskunftsberechtigten Personen nicht an den Dienstleister verweisen darf, sondern selbst handeln muss.

Das Kultusministerium empfiehlt das bei BelWue gehostete Moodle. Moodle ist eine Plattform die zu Lern-, Informations- und Kommunikationszwecken genutzt werden kann und ist aus datenschutzrechtlicher Sicht zulässig.

Die folgenden Kriterien und Hinweise helfen bei der Auswahl einer anderen geeigneten und vor allem datenschutzrechtlich zulässigen Plattform.

	Muss	Soll	Sonst.
1. Auswahl des Dienstleisters			
Bietet der Dienstleister ausreichend Gewähr für eine datenschutzgerechte Datenverarbeitung? Hierbei helfen folgende Leitfragen: • Verfügt er über Datenschutz Know-How? • Gab es in der Vergangenheit keine bei dem Dienstleister bekannt gewordene Datenschutzpannen oder techn. Missstände?	O		
Liegt eine Zertifizierung nach BSI Grundschutz oder ISO 27001, bzw. ISO 27018 vor für • die Plattform an sich, d.h. die eigentliche Anwendung / die Applikation? • das Rechenzentrum (wenn nicht durch die Schule selbst betrieben)? Siehe auch Hinweis in der nächsten Zeile		O O	
Die Schule muss sich von den vom Dienstleister getroffenen technischen und organisatorischen Maßnahmen überzeugen. Wenn die Schule nicht die Mittel und Möglichkeiten hat, die ordnungsgemäße Verarbeitung ihrer Daten beim Cloud-Anbieter zu überprüfen, könnten aktuelle und aussagekräftige Nachweise von anerkannten und unabhängigen Prüfungsorganisationen herangezogen werden. Hierzu gehört insbesondere eine Zertifizierung nach BSI-Grundschutz + Baustein Datenschutz oder ISO 27001(dann muss der Baustein Datenschutz durch die Schule geprüft werden, siehe Hinweis des KM zur Zertifizierung bei einer ADV).			Hinweis
Befindet sich der Sitz des Dienstleisters innerhalb der Europäischen Union (EU)? Eine Verarbeitung personenbezogener Daten von Schulen außerhalb der EU muss grundsätzlich unterbleiben und ist nur im Ausnahmefall (z.B. Auslandsschule) mit Zustimmung des KM zulässig.	O		
Lässt es der Dienstleister zu, dass sich die Schule von der Einhaltung der Datenschutzmaßnahmen selbst	O		

überzeugen kann? Dies kann z.B. durch eine Begehung und Prüfung des Rechenzentrums vor Ort erfolgen.			
Es gibt keine Anzeichen, dass der Dienstleister personenbezogene Daten zu Werbezwecken an Dritte übermittelt. Hinweis: Informationen über solche Übermittlungen sind meist in den Nutzungsbedingungen aufgeführt.	O		
2. Vertrag mit Auftragnehmer			
Es handelt sich aus datenschutzrechtlicher Sicht um einen sog. Auftragsdatenverarbeitung (Art. 28 EU-DSGVO).			Hinweis
Viele Dienstleister ermöglichen lediglich die Einwilligung in bzw. das Akzeptieren von vorgefertigten AGBs/Nutzungsbedingungen. In der Regel genügen solche vorgefertigte AGBs bzw. Nutzungsrichtlinien nicht den datenschutzrechtlichen Vorgaben des Art. 28 EU-DSGVO.			Hinweis
Das KM empfiehlt, einen Vertrag entsprechend der unter www.it.kultus.bw.de (http://www.it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen) oder auf dem Lehrerfortbildungsserver bereit gestellten Vorlagen abzuschließen			Hinweis
Teilt der Dienstleister konkret die eingesetzte Hardware, Software und die Art der Vernetzung mit?	O		
Benennt er, wo sich das Rechenzentrum befindet?	O		
Werden die vom Dienstleister getroffenen technischen und organisatorischen Datenschutzmaßnahmen konkret und nachvollziehbar dargestellt	O		
Existiert eine schriftliche oder elektronische Dokumentation bezüglich der Technik und Funktionalität der Plattform?	O		
Die Schule muss über alle Unterauftragsverhältnisse, sofern diese vorgesehen sind, informiert sein			Hinweis
Macht er **konkrete** Angaben über ggf. vorhandene Unterauftragsverhältnisse und werden die Unternehmen benannt?	O		
Lässt er zu, dass ggf. weitere Unterauftragnehmer nur nach Zustimmung der Schule beteiligt werden dürfen?	O		
Besitzt die Schule die vertraglich gesicherte Befugnis, dem Dienstleister hinsichtlich der Verarbeitung personenbezogener Daten Weisungen zu erteilen?	O		

Der Vertrag darf keine Aussage darüber enthalten, dass die AGBs bzw. andere Vertragsbestandteile einseitig geändert werden können.	O		
3. Technisch-funktionale Anforderungen			
Erfolgt die Kommunikation zwischen Nutzerendgerät und Plattform über verschlüsselte Verbindungen (SSL-Zugang, IPSec-VPN)?	O		
Kann der Zugang/die Anmeldung an der Plattform durch ein zusätzliches Authentifizierungsmerkmal (z.B. Hardware/Software-Token) abgesichert werden?		O	
Werden die Daten innerhalb der Plattform verschlüsselt abgespeichert?		O	
Bietet die Plattform die Funktion, Daten sicher und endgültig zu löschen?	O		
Nach welchem Datensicherungskonzept werden die in der Plattform liegenden Nutzerdaten gesichert? Hier sollte der Dienstleister das eingestellte Sicherungsverfahren darstellen.			Hinweis
Ist eine vom Nutzer veranlasste Rücksicherung einzelner Nutzerdaten (z.B. Dokumente) möglich? Entstehen hierfür keine zusätzlichen Kosten? (Ggf. mit Preisangabe)		O O	
Werden die Aufenthaltsdauer und Bewegungen der Nutzer in der Plattform protokolliert?	O		
Werden Löschfristen für diese Daten angegeben bzw. ist die Löschung technisch möglich (siehe unten Tipps für den Betrieb)?	O		
Werden die Daten einer Schule in der Plattform als Mandat geführt? Dies ist erforderlich, wenn mehrere Schulen oder andere Kunden auf einer Plattform arbeiten. Die ordnungsmäßige, getrennte Verarbeitung personenbezogener Daten in einer gemeinsamen IT-Infrastruktur muss durch zusätzliche technische und organisatorische Sicherheitsmaßnahmen sichergestellt werden. Diese sind vom Auftragnehmer darzustellen.	O		Hinweis
Gibt es eine detaillierte Rechte- und Rollenverwaltung? Welche Rollen können ggf. vergeben werden?	O		
Können in der Plattform Dokumente gespeichert werden?	O		
Kann ggf. definiert werden, für welchen Benutzerkreis diese Dokumente zur Verfügung stehen sollen?	O		

Kann die Plattform oder ein Teil ihrer Funktionen auch über eine App genutzt werden? Wenn ja: Ist die App gegen missbräuchlichen Zugriff geschützt und wie erfolgt dieser Schutz? Besteht für die Datenübertragung zwischen mobilem Endgerät und zentralem Plattform-Server eine Ende-zu-Ende Verschlüsselung? Werden die Daten auf dem mobilen Endgerät verschlüsselt gespeichert?	O O O		Hinweis
Falls Apps benötigt werden: Für welche Betriebssysteme stehen ggf. Apps zur Verfügung? iOS Android Windows sonstige		O O O O	

Sollten Antworten zu den oben genannten Aspekten nicht vorliegen oder sollte sich die Schule nicht in der Lage sehen diese Punkte zu beurteilen, so sollte von einer Beauftragung abgesehen werden.

Tipps für den Betrieb:

- Eventuell vorhandene **Foren oder Diskussionsplattformen** sollten auf keinen Fall öffentlich sein, sondern nur den Nutzern an der Schule, nach Authentifizierung zugänglich gemacht werden. Der öffentliche Zugriff auf diese Foren sollte generell deaktiviert sein. Hintergrund: Die Schule ist für sämtliche, auch von Dritten eingestellte Inhalte verantwortlich. Das bedeutet, dass die Schule permanent die Eintragungen überprüfen und ggf. löschen müsste. Das kann die Schule i.d.R. nicht leisten
- **Logs bzw. Protokolldateien** - denken Sie bitte hierbei auch an den Webserver - sollten regelmäßig gelöscht werden. Bei Webserver-logs wird eine Löschfrist von 7 bis 14 Tagen empfohlen. Ansonsten sollten 30 bis 90 Tage ausreichen.
- Sobald eine Plattform im Internet erreichbar ist, gehört diese zu dem Web-Auftritt der Schule, und muss über ein entsprechendes **Impressum** verfügen. Allgemeine Informationen zum Impressum der Homepage einer Schule finden Sie auf dem Lehrerfortbildungsserver Fallbeispiele: Impressum. Das Impressum muss schon vor der Anmeldung an der Plattform erreichbar sein.
- In den Informationen zum Datenschutz ist anzugeben, welche personenbezogenen Daten eines Betroffenen verarbeitet werden. In diesem Zusammenhang sind auch die technischen Daten anzugeben, die durch den Betrieb entstehen, z.B. die erfasste IP-Adresse oder der Zeitpunkt des An- oder Abmeldens. Des Weitern muss dargestellt werden, zu welchem Zeitpunkt die Daten

wieder gelöscht werden, und dass der Anwender das auch selbst durchführen kann, soweit die technischen Voraussetzungen gegeben sind.
Diese Informationen zum Datenschutz müssen ebenfalls vor der Anmeldung an der Plattform erreichbar sein.

- Wird an der Schule eine solche Plattform eingeführt, so ist der örtliche Personalrat zu beteiligen. Ferner sollten Schülerinnen und Schüler, sowie die Eltern informiert werden. Hierfür bietet sich der Elternabend an.

Begriffs- und Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BSI	Bundesamt für die Sicherheit in der Informationstechnik
IPSec	(Internet Protocol Security) Protokoll, welches eine gesicherte Kommunikation über potentiell unsichere Netze wie das Internet ermöglicht
ISO	Internationale Organisation für Normung
LDAP	(Lightweight Directory Access Protocol) Anwendungsprotokoll aus der Netzwerktechnik zur Abfrage und Modifikation von Informationen eines Verzeichnisdienstes (eine im Netzwerk verteilte hierarchische Datenbank) über ein IP-Netzwerk.
LDSG	Landesdatenschutzgesetz Baden-Württemberg
log-Dateien	(Protokolldatei, log file) automatisch geführtes Protokoll von Prozessen auf einem Computersystem.
Mandantenfähigkeit	Informationstechnik, die auf demselben Server oder Software-System mehrere Mandanten, also Kunden oder Auftraggeber, bedient, ohne dass gegenseitiger Einblick in ihre Daten(Benutzerverwaltung und Ähnliches) möglich ist.
SSL	(Secure Sockets Layer) hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS (Transport Layer Security) weiterentwickelt und standardisiert
VPN	(Virtual Private Network) privates (in sich geschlossenes) Rechnernetz, das auf einer öffentlichen Netzwerk-Infrastruktur (z.B. Internet) aufgebaut ist