Datenschutzrechtliche Hinweise -Vorläufig-

zur Nutzung eines Elektronischen Tage- und Klassenbuch (ETB)

I. Allgemeines

Das Klassen-, Lerngruppen- oder Kurstagebuch kann auch elektronisch geführt werden. Es besteht daneben die Verpflichtung, in regelmäßigen Abständen die gespeicherten Inhalte auszudrucken und in dieser Form zu archivieren.

II. Datenschutzrechtliche Problematik

In dem elektronischen Klassen-, Lerngruppen- oder Kurstagebuch werden personenbezogene Daten geführt, die hohe Anforderungen an den Datenschutz stellen. Der unbefugte Zugriff auf diese Daten soll mit den im Folgenden dargestellten Vorgaben verhindert werden. Sie wenden sich einerseits an den Anbieter des elektronischen Klassenbuchs, andererseits aber auch an die Schule selbst.

III. Netzinfrastruktur

Die erforderliche Netzinfrastruktur hängt davon ab, wo die Daten gespeichert werden. Bei der Gestaltung der schulischen Netzwerkinfrastruktur sind die Vorgaben des Netzbriefs in seiner aktuellsten Fassung zu beachten.

- Im Regelfall werden die Daten des elektronischen Tagebuchs nicht auf einem Server der Schule sondern bei einem Dienstleister gespeichert sein.

  Es handelt sich dann um eine sog. **"Datenverarbeitung im Auftrag"** nach Art. 28 DSGVO. Die Schule muss deshalb mit dem Anbieter eine Vereinbarung abschließen, sofern die Voraussetzungen dafür vorliegen.

- Werden die Daten **an der Schule** selbst gespeichert, muss das elektronische Tagebuch in einem eigenen physikalischen oder virtuellen Netz verortet werden. Die Verortung im „Lehrernetz“ ist nicht möglich, da ein Zugriff auf diese Umgebung vom Klassenzimmer aus unzulässig ist. Der Zugriff auf dieses eigene Netz ist so zu beschränken, dass nur auf die Bedienoberfläche des ETBs zugegriffen werden kann.

- Der Zugriff kann auch über ein eigenes, gut abgesichertes WLAN erfolgen (WPA2-Enterprise nach 802.11i mit persönlicher Authentifizierung über ein X.509-Zertifikat nach 802.1X, mind. 15 Zeichen lange, komplexe Passphrasen – WLANs mit WPA2-Personal sind nicht ausreichend).
- Die Einrichtung eines unidirektionalen Zugriffs vom Verwaltungsnetz aus ist zulässig.

IV. Verschlüsselung

Die Datenübermittlung von den Clients, also den Endgeräten, mit welchen Lehrkräfte ihre Eintragungen in das Tagebuch durchführen, zum Server muss Ende-zu -Ende verschlüsselt entsprechend dem aktuellen Stand der Technik (also z.B. AES 256bit, gültige und nicht selbst-signierte X.509-Zertifikate, …) erfolgen.

V. Authentifizierung

Im Regelfall wird die Lehrkraft die erforderliche Eingabe im Klassenzimmer vornehmen. Das Risiko, dass dabei das Passwort der Lehrkraft ausgespäht wird, ist erheblich. Es gewährleistet deshalb allein keine ausreichende Sicherheit. Erforderlich für die Nutzung des elektronischen Tagebuchs ist eine sog. "zwei Faktoren Authentifizierung" (bestehend aus "Besitz" und "Wissen"). Zusätzlich zum Passwort ist somit der Besitz eines "elektronischen Schlüssels" oder Einmal-Passworts erforderlich, auch eine TAN-Liste kann verwendet werden. Der Schlüssel kann entweder als "Clientzertifikat" auf dem jeweiligen Endgerät hinterlegt sein oder als sog. "Hardware bzw. Software-Token" z.B. über einen USB-Stick oder über eine Chipkarte (in Verbindung mit einem Lesegerät) mobil im Besitz der Lehrkraft sein.

- Bleibt das Endgerät, das für die Eingabe bestimmt ist, stationär im Klassenzimmer, scheidet die Möglichkeit der Authentifizierung über ein auf dem Computer abgelegtes **Clientzertifikat** aus, weil dann das Risiko eines unbemerkten Diebstahls zu groß ist.

  Zur Nutzung von Clientzertifikaten wird eine "Certificate Authority (CA)" benötigt, die ein solches Zertifikat vergibt und zur jeweiligen Authentifizierung verifiziert. Dabei ist darauf zu achten, dass für den Fall, dass zur CA personenbezogene Daten übermittelt werden, dies eine Datenverarbeitung im Auftrag darstellt. Es darf also kein Anbieter außerhalb der EU beauftragt werden.

  Für den Vertrag nach Art. 28 DSGVO kann die Vorlage des Kultusministeriums genutzt werden.

- Der Nutzer ist verpflichtet, das **Token** sorgsam zu verwahren und gegen Diebstahl zu schützen. Beim Hardware-Token muss sichergestellt sein, dass dieser nicht vervielfältigt werden kann.

- Der Verlust des "Schlüssels" ist vom Nutzer unverzüglich anzuzeigen, damit er für die Authentifizierung gesperrt werden kann. Er wird damit also für einen potentiellen Dieb wertlos.

- Die Authentifizierung muss über eine nach dem Stand der Technik gesicherte Verbindung erfolgen.

- Das Benutzer-Passwort muss aus mindestens zehn Zeichen bestehen und mindestens ein Sonderzeichen (wie z.B. ?, #, !) enthalten. Es sollte sowohl Groß- als auch Kleinbuchstaben sowie Ziffern enthalten. Das Passwort darf bei der Eingabe nicht am Bildschirm angezeigt werden und muss im Falle einer lokalen Installation des ETB im Computer verschlüsselt gespeichert werden. Das initial-Passwort muss nach der ersten Anmeldung geändert werden. Nach max. fünf Fehleingaben muss die zugehörige Benutzerkennung automatisch gesperrt werden.

- Bei Verwendung einer 2-Faktor-Authentifizierung auf Basis von Einmalpasswörtern (TOTP- bzw. OTP-Verfahren) ist zu deren Erzeugung ein zweites Gerät zwingend erforderlich. Dieses Gerät muss sich im persönlichen Besitz der Lehrkraft befinden. Die Lehrkraft hat für einen Zugriffsschutz entsprechend dem Stand der Technik zu sorgen

VI. Steuerung der Zugriffe - Berechtigungen

- **Zugriff von innerhalb der Schule**

  In dem elektronischen Tagebuch sind vielfältige personenbezogene Daten abgelegt, auf die nach den Vorgaben des Landesdatenschutzgesetzes nur die Lehrkräfte bzw. Mitglieder der Schulleitung zugreifen dürfen, für deren Tätigkeit diese Informationen zur dienstlichen Aufgabenerfüllung "erforderlich" sind.

  Das elektronische Tagebuch muss deshalb über ein **Rechte- und Rollenkonzept** zur Zugriffssteuerung verfügen. Dabei ist **mindestens zwischen Fachlehrkraft, Klassenlehrkraft und Schulleitung** zu unterschieden.
  Die Schulleitung hat Zugriff auf alle Eintragungen an Ihrer Schule. Klassenlehrkräfte dürfen im Rahmen ihrer Aufgabenerfüllung auf alle Eintragungen zu ihrer Klasse zugreifen und Fachlehrkräfte grundsätzlich nur auf ihre eigenen Eintragungen.

- **Zugriff von außerhalb**

  Auch Eltern sowie Schülerinnen und Schüler können ein Interesse daran haben, auf bestimmte Informationen zuzugreifen. Diese können, falls die Schule einen solchen Zugriff realisiert, Zugriff auf die eigenen Daten (Hausaufgaben und Unterrichtsversäumnisse), nicht aber auf die Eintragungen zum Unterrichtsfach, zur unterrichtenden Lehrkraft und zum Unterrichtsgegenstand erhalten. Die Authentifizierung erfolgt durch ein Passwort (s.o. Anforderungen an Passwörter).

Ein solcher Zugriff erfordert Sicherheitsmaßnahmen.

Empfehlung: die Daten, auf die Schülerinnen und Schüler sowie Eltern von außen zugreifen sollen, werden in der "DMZ", d.h. in einem separaten Netz, das gegenüber den schulischen Netzen abgeschirmt ist, abgelegt. Ein direkter Zugriff von außen auf das LAN der Schule ist zu verhindern.

VII. Protokollierungen

Eingabeprotokollierung: Es muss protokolliert werden, welche Daten zu welcher Zeit von wem in das elektronische Tagebuch eingegeben worden sind (dies umfasst die Eingabe, Veränderung und Löschung der Daten).

Zugriffs- und Übermittlungskontrolle: Es muss protokolliert werden, welcher Nutzer sich wann an das System angemeldet hat und auf welche Daten zugegriffen wurde.

Speicherkontrolle: Es ist zu empfehlen, dass sämtliche Daten in verschlüsselter Form gespeichert werden.