Datenschutzrechtliche Hinweise für den Gebrauch privater Datenverarbeitungsgeräte durch angehende Lehrkräfte zur Verarbeitung personenbezogener Daten

Art und Umfang der verarbeiteten personenbezogenen Daten orientieren sich an den herkömmlich während der Ausbildung benötigten Daten und dürfen das notwendige Maß nicht überschreiten. Besonders schutzwürdige Daten dürfen nicht auf dem privaten Datenverarbeitungsgerät verarbeitet werden.
Jedoch dürfen angehende Lehrkräfte im Rahmen ihrer Ausbildung personenbezogene Daten von Schülerinnen und Schülern für Unterrichtsentwürfe, beispielsweise für sonderpädagogische Zwecke, verarbeiten. Diese personenbezogenen Daten sind nach Fertigstellung entweder auszudrucken und/oder auf dienstliche Geräte zu übertragen und sodann auf den privaten Datenverarbeitungsgeräten unverzüglich zu löschen.
Die personenbezogenen Daten müssen durchgängig verschlüsselt gespeichert und verschlüsselt über das Internet übermittelt werden. Diese Daten sind getrennt von privaten, persönlichen Daten zu speichern und gegen unbefugten Zugriff zu schützen. Empfohlen wird eine Speicherung dienstlicher personenbezogener Daten auf einem verschlüsselten USB-Stick, um eine Trennung von dienstlichen und privaten Daten zu gewährleisten. Der Datenträger ist sorgsam zu verwahren.
Die Daten müssen spätestens nach dem Ende des nächsten Schuljahres gelöscht werden.
Jeder Verlust ist sofort der Seminarleitung zu melden, gegebenenfalls sind zudem die Melde- und Benachrichtigungspflichten entsprechend 1.10. der Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ zu beachten.

Genehmigung
Die Seminarleitung muss über Art und Umfang der vorgesehenen Verarbeitung personenbezogener Daten auf einem privaten Datenverarbeitungsgerät (PC, Laptop, Tablet, Smartphone, Wechseldatenträger wie DVD, USB-Stick, externe Festplatte …) einer angehenden Lehrkraft informiert sein und dieser Datenverarbeitung schriftlich zustimmen.
Diese datenschutzrechtlichen Hinweise sind der angehenden Lehrkraft auszuhändigen. Hierfür muss die Lehrkraft der Seminarleitung eine Übersicht der verwendeten Hard- und Software sowie eine Bestätigung der getroffenen technischen und organisatorischen Maßnahmen (Artikel 32 EU-DSGVO und § 3 LDSG) vorlegen. Das Kultusministerium stellt hierfür eine Vorlage unter www.it.kultus-bw.de zur Verfügung, die von den Schulen zu verwenden ist und analog für die Seminare eingesetzt werden kann.

Technische und organisatorische Datenschutzmaßnahmen
Diese Datenschutzmaßnahmen müssen insbesondere gewährleisten, dass ein

unbefugter Zugriff auf die Daten wirksam unterbunden wird.
Es müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- **die Pseudonymisierung und Verschlüsselung personenbezogener Daten**
  Eine Pseudonymisierung muss nur dann durchgeführt werden, wenn dies für die Aufgabenerfüllung sinnvoll ist und die Aufgabenerfüllung damit möglich ist. Sollen zum Beispiel Beratungsprotokolle verwaltet werden, ist eine Pseudonymisierung nicht sinnvoll.
  Die Daten müssen in jedem Fall durchgängig **verschlüsselt** gespeichert werden. Die Verschlüsselung kann zum Beispiel mittels der Software "VeraCrypt" durchgeführt werden.
  Werden weitere Datenträger wie zum Beispiel USB-Sticks oder externe Festplatten verwendet, müssen die dienstlichen Daten auch dort verschlüsselt sein.

- **die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;**
  Je nach Art der Informationen stehen unterschiedliche Schutzziele im Vordergrund: So muss sichergestellt werden können, dass Informationen vertraulich behandelt werden, dass sie nicht absichtlich oder versehentlich geändert werden und dass sie dann zur Verfügung stehen, wenn sie benötigt werden. Folgende Fragen sind hierbei unter anderem zu klären:
  - Wo und wie werden die Geräte verwahrt?
    Sichere Verwahrung. Zum Beispiel abschließbarer Raum oder abschließbarer Schrank ...?
  - Wie wird sichergestellt, dass das private Gerät nicht durch Unbefugte genutzt werden kann?
    Zum Beispiel geheimes Passwort für den Gerätezugang.
  - Wie wird gewährleistet, dass andere Benutzer des Gerätes, zum Beispiel Familienangehörige, nicht auf die dienstlichen Daten zugreifen können?

- Zum Beispiel durch Einrichtung verschiedener Benutzerprofile wird der Zugriff auf die dienstlichen Daten geschützt oder durch Ablage der Daten in einem speziellen Bereich des Dateisystems mit eingeschränkter Zugriffsberechtigung. Es wird empfohlen, dass das Benutzerkonto über keine administrativen Berechtigungen verfügt.
- Wenn Daten an andere Stellen oder Personen übermittelt oder transportiert werden, müssen die Daten verschlüsselt werden.
- Wohin werden welche Datenarten zu welchem Zweck übermittelt? Ist die Sicherheit der Übermittlungsmethode bekannt und angemessen?
- Wie und durch welche Software erfolgt die Verschlüsselung?
- Wie werden Daten gelöscht? Welche Software kommt zum Einsatz? Hinweise, welche Software eingesetzt werden kann, finden Sie auf der Homepage des BSI und auf dem Lehrerfortbildungsserver.

- **die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.**
  Folgende Fragen sind hierbei unter anderem zu klären:
  Auf welche Weise und wie häufig erfolgen Datensicherungen, sogenannte Backups? Werden die Daten gespiegelt? Wird ein Speichernetzwerk (SAN oder NAS) eingesetzt?

- **Ferner ist Folgendes zu beachten:**
  - Das eingesetzte Betriebssystem muss durch die Installation von Updates oder Patches regelmäßig auf dem aktuellen Stand gehalten werden.
  - Es ist generell die Möglichkeit der Authentisierung (personalisierte Anmeldung) insbesondere beim Betriebssystem zu nutzen.
  - Es ist eine Firewall einzusetzen (für den Fall dass das Gerät sich im Internet befindet) sowie eine Virenschutzsoftware. Diese sind stets auf dem aktuellen Stand zu halten.
  - Empfohlen wird, sämtliche Updates (Betriebssystem, Firewall, Virenschutz) **automatisiert** erfolgen zu lassen, dies kann durch entsprechende Konfiguration der Software erfolgen.
  - Passwörter sind so zu wählen, dass sie dem Stand der Technik entsprechen. Infos hierzu erhalten Sie auf dem Lehrerfortbildungsserver.
  - Bei der Nutzung von Webportalen darf das eingegebene Passwort nicht im Browser für weitere Sitzungen gespeichert werden. Dies verhindert die unberechtigte Nutzung des Webportals durch andere Nutzer Ihres privaten Umfelds, zum Beispiel durch im Haushalt wohnende Kinder.

- Das Löschen mit Betriebssystemmitteln reicht in der Regel nicht aus, weil Daten trotz dieser Löschung wiederhergestellt werden können.
- Die Nutzung fremder Internetzugänge (zum Beispiel in Internet-Cafes oder Hot-Spots an öffentlichen Plätzen) ist grundsätzlich verboten, es sei denn, der Internetzugang verfügt über eine Verschlüsselung. Die Nutzung des eigenen WLAN darf nur erfolgen, wenn das WLAN sicher verschlüsselt ist (zum Beispiel aktuelle WPA2-Verschlüsselung).
- Für die Speicherung und sonstige Verarbeitung auch verschlüsselter personenbezogener Daten von privaten Datenverarbeitungsgeräten aus Clouds gelten die Anforderungen nach 1.14.2. der VwV „Datenschutz an öffentlichen Schulen“ entsprechend.

Auskunftsanspruch

Die Seminarleitung und gegebenenfalls der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg haben gegenüber den angehenden Lehrkräften einen Auskunftsanspruch über die auf den privaten Geräten gespeicherten **dienstlichen** personenbezogenen Daten. Die angehende Lehrkraft muss daher schriftlich zusichern, dass sie bzw. er die Datenverarbeitungsgeräte und Speichermedien nach Aufforderung in die Räume des Seminars zu Kontrollzwecken bringen wird und eine Kontrolle der **dienstlich** verarbeiteten Daten durch dazu berechtigte Personen duldet. Dies erfolgt im Beisein der angehenden Lehrkraft.

Die angehende Lehrkraft verpflichtet sich zudem, alle zukünftigen wesentlichen Änderungen (zum Beispiel Neubeschaffung von Hardware, Einsatz neuer Software zur Verarbeitung dienstlicher personenbezogener Daten) der Seminarleitung unverzüglich mitzuteilen.

Weitere Informationen zu diesen Themen finden Sie im Internet auf der Webseite des BSI für Privatpersonen, welche unter http://www.bsi-fuer-buerger.de zu erreichen ist und unter www.lehrerfortbildung-bw.de, Rubrik Recht / Schule - Datenschutz.