Anlage 1

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

Auf privaten Datenverarbeitungsgeräten dürfen lediglich die personenbezogenen Daten jener Schülerinnen und Schüler verarbeitet werden, die von der jeweiligen Lehrkraft selbst unterrichtet werden bzw. deren Klassenlehrer bzw. Oberstufenbetreuer sie ist. Art und Umfang der verarbeiteten Daten orientieren sich an den herkömmlich etwa in einem Notenbuch geführten oder bei der manuellen Zeugniserstellung benötigten Daten. Besonders sensible Daten, etwa über Krankheiten oder Erziehungs- und Ordnungsmaßnahmen von Schülerinnen und Schülern, dürfen nicht auf dem privaten Datenverarbeitungsgerät verarbeitet werden.
Die personenbezogenen Daten müssen verschlüsselt gespeichert und verschlüsselt über 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.
Die Daten müssen spätestens nach dem Ende des nächsten Schuljahres gelöscht werden.

Genehmigung

Die Schulleitung muss über Art und Umfang der vorgesehenen Verarbeitung personenbezogener Daten auf einem privaten Datenverarbeitungsgerät (PC, Laptop, Tablet, Wechseldatenträger wie DVD, USB-Stick, externe Festplatte usw.) einer Lehrkraft informiert sein und dieser Datenverarbeitung schriftlich zustimmen. Diese Anlage ist der Lehrkraft auszuhändigen.
Hierfür muss die Lehrkraft der Schulleitung eine Übersicht der verwendeten Hard- und Software sowie eine Bestätigung der getroffenen technischen und organisatorischen Maßnahmen (§ 9 Absatz 3 Landesdatenschutzgesetz) vorlegen. Das Kultusministerium stellt hierfür eine Vorlage unter www.it.kultus-bw.de zur Verfügung.

Technische und Organisatorische Datenschutzmaßnahmen

Diese Datenschutzmaßnahmen müssen insbesondere gewährleisten, dass ein unbefugter Zugriff auf die Daten wirksam unterbunden wird.
Bei der Festlegung der zu treffenden technischen und organisatorischen Maßnahmen müssen die folgenden Aspekte berücksichtigt werden:

- **Zutrittskontrolle**
  Wo und wie werden die Geräte verwahrt?
  z.B. abschließbarer Raum oder abschließbarer Schrank, usw…?
- **Benutzerkontrolle**
  Wie wird sichergestellt, dass das private Gerät nicht durch Unbefugte genutzt werden kann?
  z.B. geheimes Passwort für den Gerätezugang

- **Zugriffskontrolle**
  Wie wird gewährleistet, dass andere Benutzer des Gerätes, z.B. Familienangehörige, nicht auf die dienstlichen Daten zugreifen können?
  z.B. durch Einrichtung verschiedener Benutzerprofile wird der Zugriff auf die dienstliche 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.
- **Datenträger und Speicherkontrolle (Verschlüsselung)**
  Wie wird sichergestellt, dass Unbefugte die gespeicherten Daten nicht lesen können?
  Die Daten müssen in jedem Fall **verschlüsselt** abgelegt werden. Wie erfolgt die Verschlüsselung, welche Software zur Verschlüsselung wird eingesetzt? Eingesetzt werden sollte die Software "TrueCrypt".
  Werden weitere Datenträger wie z.B. USB-Sticks oder externe Festplatten verwendet, müssen die dienstlichen Daten auch dort verschlüsselt sein. Welche Datenträger werden verwendet und wie erfolgt die Verschlüsselung?
- **Transportkontrolle**
  Wenn Daten an andere Stellen oder Personen übermittelt oder transportiert werden, müssen die Daten verschlüsselt werden.
  Wohin werden welche Datenarten übermittelt?
  Wie und durch welche Software erfolgt die Verschlüsselung?
- **Verfügbarkeitskontrolle**
  Auf welche Weise und wie häufig erfolgen Datensicherungen, sog. Backups?
- **Datenlöschung**
  Das Löschen mit Betriebssystemmitteln reicht i.d.R. nicht aus, weil Daten trotz dieser Löschung wiederhergestellt werden können.
  Wie werden Daten gelöscht? Welche Software kommt zu Einsatz? Hinweise, welche Software eingesetzt werden kann, finden Sie auf der Homepage des BSI und auf dem Lehrerfortbildungsserver.
- **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 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, z. B. durch im Haushalt wohnende Kinder.
  - Die Nutzung fremder Internetzugänge (z. B. 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 (z.B. aktuelle WPA2-Verschlüsselung).
  - Für die Speicherung und sonstige Verarbeitung auch verschlüsselter personenbezogener Daten von privaten Datenverarbeitungsgeräten aus Clouds gelten die Anforderungen nach Nr. I 12.2 dieser Verwaltungsvorschrift.

Auskunftsanspruch

Die Schulleitung und ggf. der Landesbeauftragte für den Datenschutz hat gegenüber der Lehrkraft einen Auskunftsanspruch über die auf den privaten Geräten gespeicherten **dienstlichen** personenbezogenen Daten. Die Lehrkraft muss daher schriftlich zusichern, dass sie die Datenverarbeitungsgeräte und Speichermedien nach Aufforderung in die Räume der Schule zu Kontrollzwecken bringen wird und eine Kontrolle der **dienstlich** verarbeiteten Daten durch dazu berechtigte Personen duldet.

Die Lehrkraft verpflichtet sich zudem, alle zukünftigen wesentlichen Änderungen (z.B. Neubeschaffung von Hardware, Einsatz neuer Software zur Verarbeitung dienstlicher personenbezogener Daten) der Schulleitung 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.
.

Anstelle der Hinweise auf das LDSG gilt für Katholische Einrichtungen §26 (KDG).