Hinweise für Lehrkräfte zur Umsetzung des Erlasses

Bei der dienstlichen Nutzung privater IT-Systeme sind Lehrkräfte an rechtliche Vorgaben gebunden, die sowohl die Verarbeitung personenbezogener Daten als auch deren Speicherung und Sicherung betreffen.

Die folgenden Erläuterungen sollen Lehrkräfte bei der Umsetzung des Erlasses unterstützen, um den datenschutzkonformen Einsatz privater IT-Systeme zur Erledigung dienstlicher Aufgaben zu gewährleisten.

Was gilt für alle IT-Systeme in gleicher Weise?

- Zunächst muss die dienstliche Nutzung privater IT-Systeme vorab durch die Schulleitung genehmigt werden. Das dafür benötigte Formular ist in den Schulen verfügbar.
- Lehrkräfte dürfen nach Genehmigung mit ihren privaten IT-Systemen personenbezogene Daten verarbeiten und auf einem gesicherten Server der Schule speichern. Die Datenspeicherung auf dem Server eines Fremdanbieters ist zulässig, sofern die Schule einen entsprechenden Vertrag zur Auftragsdatenverarbeitung geschlossen hat[1].
- Die Genehmigung gilt für einen Zeitraum von fünf Jahren; danach ist ggf. erneut eine Genehmigung zu beantragen. Bei wesentlichen Änderungen, wie z. B. dem Austausch des IT-Systems, dem Wechsel des Betriebssystems oder dem Einsatz zusätzlicher Anwendungssoftware ist unverzüglich eine neue Genehmigung zu beantragen. Bei einem Update des Betriebssystems, dem Wechsel zu einer neuen Version oder dem Update bereits genehmigter Anwendungssoftware ist keine neue Genehmigung erforderlich.
- Updates und Patches für die genutzte Hard- und Software sollten möglichst automatisch eingespielt werden, um die Gerätekonfiguration aktuell zu halten.
- Die elektronische Übersendung personenbezogener Daten sowie deren Transport mittels elektronischer Speichermedien sind nur zulässig, wenn die Daten verschlüsselt werden. Bei einer Datenübermittlung über das Internet ist ein verschlüsselter Transportweg einzuhalten. Die Transportverschlüsselung ist mittlerweile Standard bei der Nutzung von Internetangeboten. Erkennbar ist sie an dem Kürzel „https://“ am Anfang einer Internetadresse. Üblicherweise schalten Webseiten automatisch auf „https://“ um, wenn sie ohne dieses Kürzel aufgerufen werden.

Welche besonderen Regelungen gibt es für IT-Systeme mit den Betriebssystemen iOS/iPadOS, Android (inklusive davon abgeleiteter Betriebssysteme) oder ChromeOS?

- Die Speicherung personenbezogener Daten auf dem Festspeicher privater mobiler Endgeräte (Smartphones und Tablets) im Sinne der Ziffer 1.1 des Erlasses ist nicht zulässig.

---

[1] Dieser Vertrag muss den Vorgaben der Artikels 28 sowie 44-49 der Datenschutz-Grundverordnung (DSGVO) entsprechen. Anbieter von Cloud-Diensten legen den Schulen üblicherweise einen DSGVO-konformen Vertrag zur Unterzeichnung vor.
Es liegt in der Verantwortung der Schule, einen geeigneten Anbieter auszuwählen und mit der Datenverarbeitung im Auftrag zu betrauen. Wegen dieser besonderen Rolle der Schule können Lehrkräfte keine separaten Verträge zur Auftragsdatenverarbeitung schließen.
Anbieter mit Geschäftstätigkeit in den USA, die den Bestimmungen des CLOUD-Act unterliegen, können die Anforderungen der DSGVO in der Regel nicht erfüllen.

Darunter sind Endgeräte zu verstehen, auf denen nicht die Betriebssysteme Windows, MacOS oder Linux installiert sind. Vor allem die Betriebssysteme iOS/iPadOS, Android (inklusive weiterer Betriebssysteme auf Basis von Android) oder ChromeOS werden auf solchen Geräten genutzt.

- Datensicherungsmaßnahmen:
  Das Gerät ist vor unberechtigter Nutzung zu schützen, beispielsweise durch eine automatische Sperrung des Startbildschirms und Entsperrung mittels PIN-Code.
  Die Zugangsdaten zum gesicherten Server der Schule oder einer beauftragten Stelle i. S. d. Art. 28 der Datenschutz-Grundverordnung (DSGVO) dürfen nicht auf dem Endgerät gespeichert werden.

Welche besonderen Regelungen gibt es für IT-Systeme mit den Betriebssystemen Windows, MacOS oder Linux?

- Private (stationäre oder mobile) Endgeräte mit den Betriebssystemen Windows, MacOS oder Linux fallen nicht unter das Verbot der Speicherung personenbezogener Daten auf dem Festspeicher.
- Datensicherungsmaßnahmen:
  Werden die Daten auf internen Speichermedien (z. B. Festplatte) abgelegt, sind die Daten durch geeignete technische Maßnahmen gegen Zugriff zu sichern. Dafür ist mindestens
    - eine Zugriffskontrolle durch das Betriebssystem auf Verzeichnis- oder Dateiebene einzurichten sowie
    - eine Verschlüsselung der Verzeichnisse, in denen die Daten gespeichert sind, vorzunehmen.

  Diese Sicherung gegen unbefugten Zugriff wird mit der Erstellung eines separaten passwortgeschützten Benutzerkontos eingerichtet.
  Die Verschlüsselung muss nicht für das gesamte Speichermedium eingerichtet werden. Es können die Daten auch in einem genügend großen Container verschlüsselt auf dem Speichermedium abgelegt werden.

  Online-Zugriffe auf die Daten sind durch dem Stand der Technik entsprechende Vorkehrungen (z. B. Firewall) auszuschließen.
  Im Betriebssystem Windows sowie im MacOS ist ab Werk eine Firewall installiert und aktiviert. Unter Linux (beispielsweise Ubuntu-Desktop) ist keine Firewall erforderlich, da standardmäßig keine Ports nach außen geöffnet sind.
- Werden für die Speicherung der Daten externe Speichermedien (z. B. USB-Sticks) verwendet, sind diese zu verschlüsseln und so aufzubewahren, dass sie nur der Lehrkraft selbst zugänglich sind. Es muss nicht der gesamte Datenträger verschlüsselt werden. Es können die Daten auch in einem genügend großen Container verschlüsselt auf dem Speichermedium abgelegt werden.
- Schutz vor Schadsoftware:
  Auf Endgeräten mit dem Betriebssystem Windows besteht nach wie vor ein Bedarf für eine Antiviren-Software. Die in das Betriebssystem integrierte Software (Windows Defender) bietet einen hinreichenden Schutz.
  Das gilt auch für MacOS (Xprotect). Unter Linux ist aufgrund der besonderen Betriebssystem-Architektur ein Virenscanner nicht unbedingt erforderlich.

- Datensicherung:
  Es muss sichergestellt sein, dass die gespeicherten Daten jederzeit auch dann verfügbar sind, wenn das IT-System ausfällt oder der Datenträger beschädigt wird. Bei Endgeräten mit dem Betriebssystem Windows ist die entsprechende Funktionalität mittlerweile integriert und kann über die Systemsteuerung eingerichtet werden.
  Unter MacOS ist die Funktionalität ebenfalls bereits vorhanden (Time Machine). Unter Linux (Ubuntu-Desktop) ist diese Funktion ebenfalls schon vorinstalliert („Datensicherungen“).

Weitere technische Hinweise und Anleitungen zum sicheren Betrieb privater IT-Systeme unter Windows, MacOS und Linux finden Sie im Datenschutzportal https://datenschutz.nibis.