Hinweise zum Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke

SACHSEN-ANHALT

Landesschulamt

Bei der Genehmigung der Nutzung privater Geräte und der Gewährleistung der technischen und organisatorischen Sicherheit der Verarbeitung ist u. a. Folgendes zu berücksichtigen:

- Die Genehmigung sollte befristet sein (max. 5 Jahre). Bei wesentlichen Änderungen, insbesondere in Bezug auf die eingesetzten Geräte bzw. Betriebssysteme und wesentlichen Programme, ist unmittelbar eine Erneuerung erforderlich.

- Werden Verarbeitungsvorgänge mit privaten Geräten der Lehrkräfte durchgeführt, ist zu prüfen, ob sich dies in die Verarbeitungsvorgänge der Schule integriert (z. B. Webzugriff auf Programm auf dem Schulserver bzw. Nutzung des Programms des Auftragsverarbeiters der Schule) oder ob ggf. von einem eigenständigen Verfahren auszugehen ist, für das gesondert ein Verzeichnis der Verfahrenstätigkeiten erstellt werden muss (Art. 30 DS-GVO).

- Für den Zugriff auf zentral gespeicherte schulische Datenbestände ist die Zugriffsberechtigung im Rahmen der jeweiligen konkreten Erforderlichkeit zu regeln (Berechtigungskonzept). Durchgeführte Verarbeitungsvorgänge wie insbesondere Änderungen, Abfragen und Übermittlungen sind zur Nachvollziehbarkeit zu protokollieren.

- Die für die Verarbeitung von Schülerdaten genutzten Datenverarbeitungsgeräte müssen über ein aktuelles Betriebssystem verfügen, welches durch regelmäßige Sicherheitsupdates aktualisiert wird. Für den Anschluss an das Internet ist eine Firewall zu installieren, die den Zugriff Unbefugter auf das Datenverarbeitungsgerät und die ggf. hier gespeicherten Schülerdaten verhindert. Ebenso ist ein leistungsfähiger Virenscanner zu installieren, der täglich aktualisiert werden muss.

- Personenbezogene Daten sind aus Sicherheitsgründen nach dem Stand der Technik mit anerkannten Algorithmen und ausreichenden Schlüssellängen verschlüsselt zu speichern.

- Auch beim Transport von Schülerdaten zwischen der Schule und dem privaten Arbeitsplatz der Lehrkraft ist insbesondere der Zugriff Unbefugter zu verhindern. Zur Gewährleistung eines hinreichend sicheren Transports kommen in Betracht. (z. B. verschlüsselter USB-Stick, verschlüsselte Daten auf dem Laptop, verschlüsselte Verbindung vom Endgerät zum Server).

- Bei lokaler Speicherung auf dem privaten Datenverarbeitungsgerät ist darüber hinaus durch einen entsprechenden Zugriffsschutz (z. B. Festlegung von Zugriffsrechten durch das Betriebssystem in Bezug auf Verzeichnisse oder Dateien oder Passwortvergabe zum Öffnen von Dateien) sicherzustellen, dass Unbefugte keinen Zugang zu den Schülerdaten erhalten. Für die Authentifizierung des Nutzenden für die schulische Anwendung bzw. Zugriff auf die schulischen Daten reicht eine standardmäßige 4-stellige PIN wie bei einem Smartphone üblich nicht. Durch angemessene Maßnahmen im Einzelfall wird die Vertraulichkeit der Schülerdaten gewährleistet. Die Maßnahmen sollten auch im Hinblick auf die Nachweispflicht vorab schriftlich festgelegt werden.

- Bei der Passwortgestaltung ist darauf zu achten, dass das Passwort nicht leicht zu erraten ist. Namen, Kfz-Kennzeichen, Geburtsdaten usw. dürfen deshalb nicht als Passwörter gewählt werden. Ein Passwort sollte mindestens 8 Zeichen lang sein und aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Zeichenarten verwendet werden. Es darf anderen Personen, die Zugang zu dem Gerät haben, nicht bekannt sein. Das Speichern des Passwortes auf einem mobilen Gerät sollte unterbleiben, da im Verlustfall Gerät und Passwort auf den neuen Besitzer übergehen.

- Beim Zugriff durch private Geräte auf andere Rechner (Schulserver, Cloud) sind sichere Anmeldeverfahren erforderlich, die unbefugte Zugänge verhindern. Die Identität des Nutzers muss durch sichere Authentifizierungsverfahren gewährleistet werden.

- Soweit schulische Kommunikation per E-Mail erfolgen soll, sollte ein dienstliches E-Mail-Konto verwandt werden. Die Nutzung des privaten E-Mail-Kontos der Lehrkraft führt zu einer kaum zu kontrollierenden Vermischung privater und dienstlicher Daten. Es müsste dann auch eine vorherige Einwilligung der Lehrkraft zum Zugriff auf das private E-Mail-Konto durch die Schulleitung und den Landesbeauftragten für den Datenschutz zu Kontrollzwecken geben. Die E-Mail-Kommunikation bedarf zumindest einer Transportverschlüsselung, bei sensiblen Daten der Schülerinnen und Schüler je nach dem Ergebnis der gebotenen Risikoabwägung einer Ende-zu-Ende-Verschlüsselung.

- Die Schülerdaten sind regelmäßig auf einem Backup-Medium (z. B. verschlüsselter USB-Stick) zu sichern, welches vom Datenverarbeitungsgerät bzw. dem originären Speichermedium örtlich getrennt aufbewahrt werden muss. Durch diese Maßnahme wird die Verfügbarkeit der Schülerdaten gewährleistet, indem sichergestellt wird, dass die Schülerdaten auch bei Verlust oder Zerstörung der Originaldaten zeitnah zur Verfügung stehen.

- Soweit Daten nicht in eigenen, sondern in Einrichtungen anderer Stellen verarbeitet werden (z. B. Cloudspeicher), sind die gemäß Art. 28 DS-GVO gebotenen Verträge zur Auftragsverarbeitung mit dem dort vorgegebenen Inhalt zu schließen.

- Soweit Programme verwendet werden, die Verarbeitungsprozesse in Drittstaaten durchführen, ist zunächst die Einhaltung der Vorgaben der Art. 44 ff DS-GVO zu gewährleisten (siehe zu Frage 26.). Weiter ist sicherzustellen, dass durch die Standardkonfiguration eventuell systemseitige verursachte Übermittlungen in Drittstaaten durch entsprechende Maßnahmen weitestgehend abgestellt sind.

- Für eine durchzuführende Löschung ist eine physikalische Löschung geboten, d. h. die Daten sind so zu überschreiben, dass sie nicht wiederhergestellt werden können. Für dieses „sichere“ Löschen steht eine Vielzahl von Programmen zur Verfügung. Es reicht nicht, die Daten in den Papierkorb zu verschieben und diesen anschließend zu leeren.

- Zur Gewährleistung von Kontrollen durch die Schulleitung oder den Landesbeauftragten für den Datenschutz muss eine Erklärung vorliegen, wonach die Lehrkraft und ggf. durch das Wohnungsgrundrecht mit Geschützte ein jederzeitiges Betretungsrecht gewähren, das den Zugang zum häuslichen Arbeitsplatz und zum genutzten Gerät gestattet.