

Verarbeitung von Schüler- oder Elterndaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte

Rechtliche Rahmenbedingungen

Mit der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen in der Fassung vom 4. Februar 2009 hat das Hessische Kultusministerium eine modernisierte Rechtsgrundlage für die Datenverarbeitung in Schulen geschaffen.

In § 1 Abs. 5 und § 3 werden hier die grundlegenden Voraussetzungen für die Verarbeitung der Daten von Schülern und Eltern auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte und in der Anlage 6 der Katalog der zu verarbeitenden Daten vorgegeben.

Ergänzend dazu werden durch den [Erlass zur Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrkraft](#) einzelne Bedingungen genannt, die erfüllt sein müssen, damit der häusliche Arbeitsplatz den Anforderungen an IT-Sicherheit und Datenschutz genügt.

Die Verantwortung für die Daten verbleibt auch dann bei der verarbeitenden Stelle (der Schule), wenn die Daten wegen der besonderen Beschäftigungsbedingungen der Lehrkräfte in deren häuslichem Umfeld verarbeitet werden.

Zulässig ist eine häusliche Datenverarbeitung nur dann, wenn sie sich an den sonst üblichen Standards für die Datenverarbeitung außerhalb der Daten verarbeitenden Stelle orientiert. Maßgeblich sind hier die Rahmenbedingungen, die in der [Vereinbarung zur dauerhaften Einführung alternierender Telearbeit im Bereich der Hessischen Landesverwaltung](#) festgelegt sind.

Langfristig ist daher anzustreben, dass die Daten der Betroffenen, wie in anderen Verwaltungen auch, nur auf dienstlichen Geräten verarbeitet werden, bei denen eine stärkere Kontrolle aller sicherheitsrelevanten Aspekte möglich und eine Mitbenutzung durch andere Haushaltsangehörige ausgeschlossen ist.

Bis dahin soll dem Stand der Technik entsprechend eine Speicherung der Daten auf den Festplatten oder anderen Speichern der privaten Arbeitsplatzrechner durch die Regelungen technisch und organisatorisch unterbunden werden.

Durch diese Maßnahme kann das Risiko für einen unbefugten Zugang zu den Daten erheblich gesenkt werden.

Technisch-organisatorische Maßnahmen

Der Erlass fordert daher konsequent, dass die Speicherung der personenbezogenen Daten auf einem separaten verschlüsselten Datenträger erfolgt, der ausschließlich für diese Zwecke verwendet wird.

Neben den hier genannten USB-Geräten ist auch eine durch Verschlüsselung und Zugriffsmechanismen geschützte individuelle (Lehrkraft-bezogene) Speicherung der Daten auf einer ggf. vorhandenen Plattform der Schule oder des Schulträgers möglich.

Bei der zur Verschlüsselung verwendeten Software für die USB-Komponenten, ist darauf zu achten, dass ein sicherer Algorithmus verwendet wird und dass Dateien möglichst nicht einzeln verschlüsselt werden, sondern besser in einem verschlüsselten Container, und damit in einem nur für den jeweils Berechtigten einsehbaren Verzeichnis abgelegt werden.

Allgemeine Schüler- und Elterndaten

Zum Schutz der Schüler- und Elterndaten mit normalem Schutzbedarf nach Anlage 6 Punkt 1-13 der Rechtsverordnung vor unbefugtem Zugriff und zur Sicherstellung der Verfügbarkeit sind die Lehrkräfte durch die Schulen über die Verarbeitungsbedingungen zu unterrichten und auf die Einhaltung der folgenden organisatorischen und technischen Maßnahmen zu verpflichten:

Die Lehrkräfte melden die Verarbeitung der Daten bei ihrer Schule an und hinterlegen für Notfälle das persönliche Passwort für die Verschlüsselung in einem verschlossenen Umschlag, der in der Schule gesichert aufbewahrt wird.

Arbeitsergebnisse sind zeitnah auf die Systeme der Schulverwaltung zu übertragen. Werden Arbeiten in mehreren Schritten vervollständigt oder über längere Zeiträume fortgeführt, sind dort auch regelmäßig Sicherungskopien zu hinterlegen.

Daten, die nach der Übertragung in die Systeme der Schulverwaltung nicht mehr lokal benötigt werden, sind, **soweit die Aufbewahrung nicht explizit geregelt ist**, unverzüglich zu löschen. Wenn aus vorhandenen Schriftstücken durch Löschen der Personenbezüge Textbausteine gewonnen werden, ist darauf zu achten, dass die personenbezogenen Daten nicht über die Historiefunktion der Office-Software mitgespeichert werden.

Der häusliche Arbeitsplatz ist so einzurichten, dass Daten und Unterlagen von Unbefugten nicht eingesehen werden können.

Sämtliche Unterlagen sind außerhalb der Bearbeitungsphase verschlossen aufzubewahren.

Es ist den Lehrkräften untersagt, die verarbeiteten Daten auf den lokalen Festplatten ihres Systems oder anderen Datenträgern oder Plattformen, als den dafür vorgesehenen, abzulegen. Um sicher zu stellen, dass auch nach Programmabstürzen keine unbemerkten lokalen Kopien entstehen, müssen die temporären Verzeichnisse nach jeder Verarbeitung überprüft und ggf. bereinigt werden. Unerledigte Druckaufträge sind zu löschen.

Wird die Bearbeitung unterbrochen, ist der Zugang zum Rechner und insbesondere zu den Daten zu sperren. Ggf. ist eine Benutzerabmeldung durchzuführen. Zusätzlich ist die automatische Sperrfunktion mit Passwortschutz am Bildschirmschoner auf eine Inaktivität von höchstens 15 Minuten Dauer einzustellen.

Der eingesetzte Rechner muss durch einen tagesaktuellen Virenschoner geschützt werden.

Ist der Rechner in ein privates Netzwerk eingebunden, sind unbefugte Zugriffe durch geeignete Konfigurationen oder durch physikalisches Trennen auszuschließen. Bei besonders gefährdeten Schnittstellen, wie WLAN sind sichere Verschlüsselungsmechanismen zu aktivieren.

Während der Verarbeitung der unverschlüsselten Daten am häuslichen System muss jede Verbindung in das Internet aktiv unterbrochen werden.

Sonderpädagogische Gutachten

Bei den in § 3 Absatz 4 der Rechtsverordnung genannten Daten (s. auch Anlage 6 Punkt 14), die im Zusammenhang mit der Erstellung von sonderpädagogischen Gutachten anfallen, ist ein höherer Schutzbedarf gegeben.

Gerade für die Verarbeitung dieser Daten ist der Einsatz dienstlicher Geräte anzustreben.

Wenn dies nicht zu realisieren ist, sind für das Erstellen von Fördergutachten mit privaten Geräten Verfahren zu wählen bzw. zu entwickeln, die jede Speicherung der Daten auf den privaten Datenverarbeitungsgeräten der Lehrkräfte weitgehend technisch ausschließen und deren Wirkung nicht von einem störungsfreien Betrieb und der Umsetzung organisatorischer Maßnahmen abhängig ist.

Daher dürfen die oben beschriebenen, plattformbasierten Lösungen in diesem Fall keine Download-Funktion haben, damit die Fördergutachten nicht auf das lokale System übertragen werden können. Zwischen den Prozessen auf der Plattform und dem lokalen System ist dann auch ein "Kopieren und Einfügen" zu unterdrücken, wie es z.B. bei Terminalserver-Lösungen möglich ist. Ein Ausdruck der Fördergutachten kann dann ausschließlich in der Schule an einem Drucker erfolgen, der über eine entsprechende netztechnische Anbindung mit der Plattform verbunden ist.

USB-Geräte kommen hier nur in Boot-fähiger Ausführung in Betracht. Dabei ist durch den Bootvorgang sicherzustellen, dass die lokalen Speichermedien, wie z.B. die Festplatte oder die Netzwerk-Schnittstellen, nicht in die Systemumgebung eingebunden werden. Eine Bearbeitung der Fördergutachten erfolgt dann zwingend nur auf dem zugelassenen USB-Gerät im verschlüsselten Container. Darüber hinaus kann noch die Schnittstelle zum Drucker aktiviert werden, damit die in der Rechtsverordnung vorgesehene Endfassung des Dokumentes erstellt werden kann.

Stand: 14.09.2009

Recherchiert und im Layout verändert am 04.11.2014;

Gefunden unter www.datenschutz.hessen.de/ds010.htm