Datenschutz in Zeiten von Corona – ein Überblick

Heiko Geiss

© Christian Horz/iStock/Getty Images Plus

Seit über 6 Monaten haben uns Einschränkungen und Folgeerscheinungen der COVID-19 Pandemie fest im Griff. Unsere Schulen versuchen sich den schwierigen Bedingungen des Fernlernunterrichts zu stellen und dabei jede Hürde zu nehmen.

Die Erreichbarkeit der Schülerinnen und Schüler sowie die nicht vorhandene technische Ausstattung oder auch die digitalen Kompetenzen der Lehrkräfte stehen dabei täglich im Fokus. Zeitgleich stehen durch Soforthilfen und Digitalpakt weitreichende Mittel zur Verfügung, bei welchen zunächst Abrufverfahren durchlaufen und Lieferschwierigkeiten überwunden werden müssen.

Verantwortliche Lehrkräfte und Schulleitungen finden sich in einem engen Korridor zwischen erlaubten und umsetzbaren Maßnahmen wieder, welcher bereits vor der Pandemie durch eine verstärkte Aufmerksamkeit gegenüber dem Datenschutz abgesteckt war. Im Folgenden erhalten Sie eine Orientierung zu häufigen Anwendungsfällen und pragmatische Ansätze zur Handhabung von Werkzeugen im Fernunterricht.

1. Datenschutz schützt nicht Daten, sondern Menschen

Zunächst ist es hilfreich, das Augenmerk nicht auf technische Umsetzbarkeiten oder die vielfältigen zur Verfügung stehenden Möglichkeiten digitaler Angebote zu legen. Im Mittelpunkt sollten die zu schützenden Personen stehen, welche sich im Verantwortungsbereich der Schule befinden. Die DSGVO gibt dazu zwei hilfreiche Ansätze, um persönlichen Schaden Betroffener abzuschätzen und gleichzeitig zu vermeiden. Im Besonderen stehen hier die *Datenschutz-Folgenabschätzung* sowie die *Ergreifung von technischen und organisatorischen Maßnahmen* im Mittelpunkt. Was könnte im schlimmsten Fall wem passieren? Wie wahrscheinlich ist der Eintritt einer Annahme und was kann im Vorfeld zur Vermeidung von Schäden getan werden? So sollten folgende Überlegungen zu einem klaren Urteil über die Verantwortbarkeit und Zulässigkeit führen:

Welche Folgen gilt es zu bedenken, wenn Lehrkräfte über ihre private E-Mail-Adresse dienstlich kommunizieren?

Besonders schützenswerte Daten wie Kontakte, vertrauliche Inhalte, Leistungsnachweise und Anhänge landen in Mailboxen und auf Servern großer Konzerne, welche mit diesen Daten Handel betreiben. Der vorgeschriebene Schutzbereich personenbezogener Daten wird somit klar verletzt. Durch die Nutzung privater Mailboxen für den dienstlichen Gebrauch erlassen diese Daten die Schule, was einer Weitergabe entspricht, für welche es keine Rechtsgrundlage gibt.

Die Schlussfolgerung muss also zu einer Maßnahme führen, welche leider noch immer nicht an allen Schulen umgesetzt wurde, nämlich die Einführung dienstlicher E-Mail-Adressen für alle Lehrkräfte, z.B. durch den Schulträger oder der zuständigen Landesbehörde. Da praktisch alle digitalen Werkzeuge, welche online genutzt werden, eine Registrierung voraussetzen, würde hier auch ein guter Beitrag zur Infrastruktur geleistet werden. Lehrkräfte können berufliche Adressen für Registrierungen auf Webseiten nutzen und bilden eine gute, unter Umständen auch öffentliche Erreichbarkeit ab. Bei entsprechender Konfiguration der Verschlüsselungstechnologie wären sogar eine vertrauliche Kommunikation oder Austausch sensibler Daten möglich. Diese könnte allerdings auch durch verschlüsselte Anhänge realisiert werden. Programme wie VeraCrypt/TrueCrypt oder 7-Zip sind hierbei sehr gut einsetzbar und stehen kostenlos zur Verfügung. Auch in Office integrierte Verschlüsselungs-Funktionen sind brauchbar, soweit die Software-Version aktuell ist.

Sollten Lehrkräfte und Schülerschaft dazu angehalten werden private Endgeräte zu verwenden, um Anwendungen wie Messenger, Videokonferenztools oder Unterrichtswerkzeuge zur Verwaltung zu nutzen?

Die Frage ist nicht zu bejahen, die Verfügbarkeit allen Überlegungen voranzustellen. Schnell landet man bei der Zählung welches Kind ein eigenes Smartphone besitzt und welche Lehrkraft über ein eigenes Tablet oder sogar ein dienstliches Notebook verfügt. Das Delta entscheidet schlussendlich dann über den Einsatz einer wie auch immer gearteten Softwarelösung und schon scheint die Kommunikationsbrücke zwischen Lehrkräften, Klassenverbänden und sogar Eltern geschlagen zu sein, denn die Mehrheit hat ja irgendein Gerät zur Verfügung.

Die Problematik, dass auch stabile und für den Nutzer kostenfreie Internetverbindungen zur Verfügung stehen müssen, offenbart sich erst in einer zweiten Überlegung und hier fällt das Delta deutlich größer aus. Kinder haben oft nur das Datenvolumen Ihrer Prepaidkarten zur Verfügung, welches bereits nach 10 bis 30 Minuten Videokonferenz aufgebraucht sein könnte und damit hohe Kosten

verursacht. Viele wissen auch ohne Hinweise darauf gar nicht um den technischen Unterschied zwischen WLAN- und Mobilfunkverbindungen, bzw. wie Ihr Smartphone einzustellen ist. Schulen stellen oftmals – wenn überhaupt – nur WLAN für Lehrkräfte zur Verfügung und haben keine BYOND Lösung. Bei mehreren hundert Nutzern (oder wenigen Nutzern mit einem hohen Upload-Bedarf) im Haus reicht die Bandbreite der zur Verfügung stehenden Internetleitung der Schule nicht aus. Der Zustand der privaten Endgeräte in Bezug auf installierter Software und vor allem Sicherheit ist nicht abschätzbar. Schaut man genauer hin, dann stolpert man bei den Smartphones der Kinder stets über rechtliche Fragen. WhatsApp ist beispielsweise erst ab 16 Jahren zulässig und sehr viele Tätigkeiten am Smartphone sind von den Eltern abzusegnen (Apps installieren). Leider werden nur wenige Geräte tatsächlich seitens der Erziehungsberechtigten überwacht oder überhaupt gesehen. Jede Verwendung seitens der Schule muss hingegen rechtlich absolut einwandfrei erfolgen. Außerdem provoziert die private wie schulische Verwendung ein und desselben Gerätes klare Verstöße gegen die DSGVO.

Wichtig

Zu schützende Daten…

- werden zwangsläufig miteinander vermischt
- aus der Zwischenablage werden aus Versehen falsch eingefügt (und unter Umständen in den Schulmessenger gepostet, vgl. copy & paste)
- verbleiben auf dem Gerät, obwohl Löschfristen zu beachten sind
- werden in Backups auf Cloudspeichern abgelegt und dort vergessen
- sind unverschlüsselt abrufbar und gelangen in die Hände Dritter bei Weitergabe bzw. bei einem Besitzerwechsel
- werden in geteilten Kontaktdatenlisten veröffentlicht und unwissentlich weitergegeben z.B. via Google Contacts,

Dies sind nur einige, aber gravierende Verstöße bei einer unreflektierten Nutzung privater Geräte. **Vor allem Lehrkräfte müssen also nach Möglichkeit unbedingt mit Geräten zur Erfüllung Ihrer unterrichtlichen Tätigkeiten ausgestattet werden**.

Was muss beim Einsatz von Software beachtet werden, falls keine digitalen Endgeräte zur Verfügung gestellt werden können?

Die eingesetzte Software läuft entweder in Form einer App auf einem privaten Gerät, wie zum Beispiel einem geeigneten und datenschutzkonformen Messenger, einer Stundenplan-App oder einem Videokonferenztool, bzw. einer App oder eingesetzten Lernplattform. Oder der Browser wird als Oberfläche genutzt, um sich für einen bestimmten Dienst (Chat, Webinar, Cloud) anzumelden.

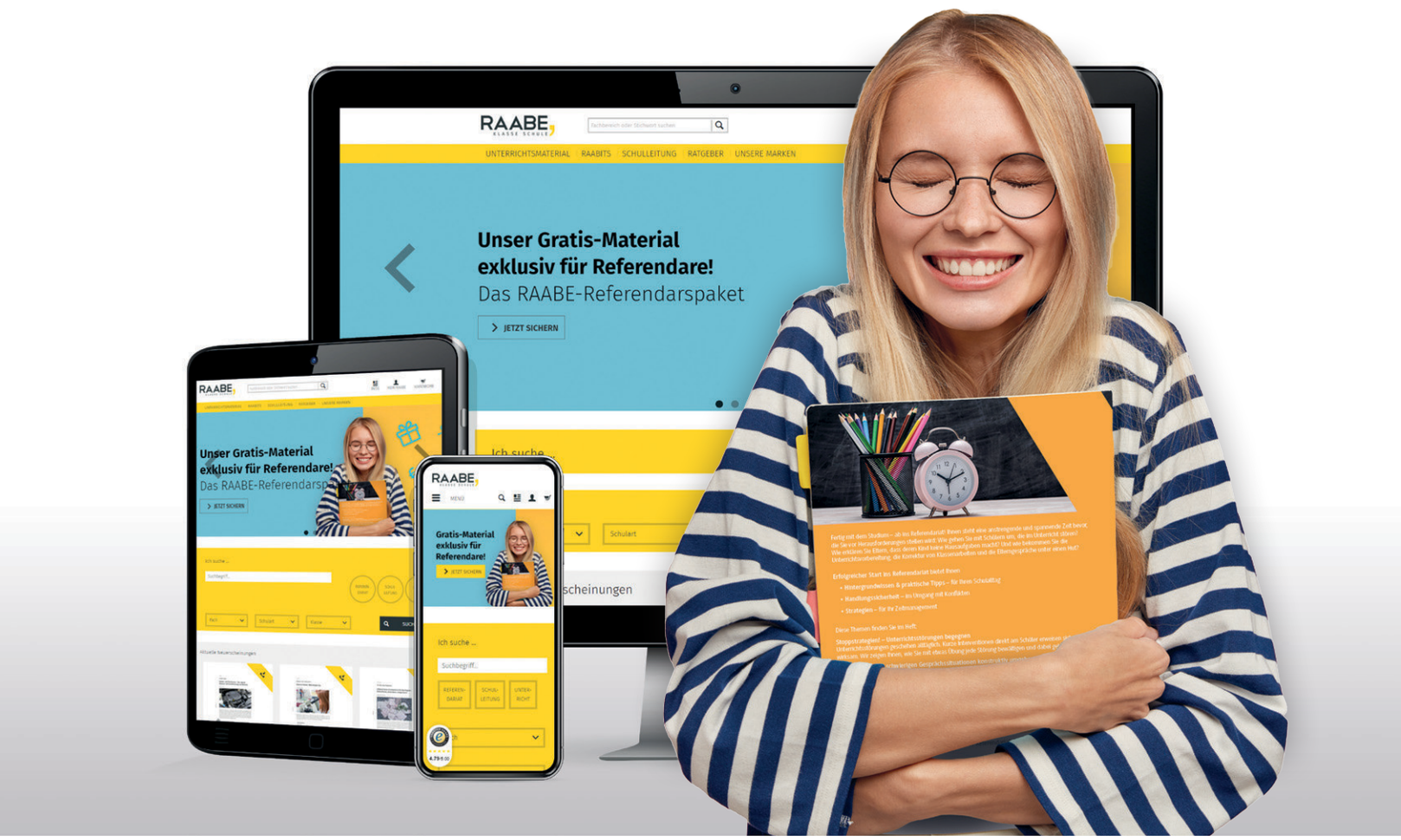
Eine einfache, aber eingeschränkte Lösung wäre die Veröffentlichung von Aufgaben für den Heimunterricht über die Schulhomepage oder über einen geteilten Link. Da hier weder personenbezogene Daten verwendet werden müssen, noch ein direkter digitaler Rücklauf verwirklicht wird, gibt es kaum Dinge bei der Umsetzung zu beachten. Die Aufgaben können von den Lehrkräften rechtzeitig bereitgestellt werden und stehen dann nach Pflege der Homepage sofort zur Verfügung.

RAABE
KLASSE SCHULE

Sie wollen mehr für Ihr Fach?

Bekommen Sie: Ganz einfach zum Download

im RAABE Webshop.



- **Über 5.000 Unterrichtseinheiten** sofort zum Download verfügbar
- **Webinare und Videos** für Ihre fachliche und persönliche Weiterbildung
- **Attraktive Vergünstigungen** für Referendar:innen mit bis zu 15% Rabatt
- **Käuferschutz** mit Trusted Shops

Jetzt entdecken:

www.raabe.de