Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

05. Juli 2021

# Zehn Bedenken gegen den Einsatz von außereuropäischen Software-Anwendungen an Schulen

Die Digitalisierung der Schulen ist eine große Herausforderung. Dies betrifft auch die Auswahl und Nutzung von Videokonferenzsystemen, von Software-Produkten und Social Media-Plattformen. Die gängigsten Produkte stammen regelmäßig aus Drittstaaten außerhalb der EU, insbesondere aus den USA. In den vergangenen Monaten und Wochen sind zahlreiche Lehrkräfte, Schülerinnen und Schüler sowie Eltern(vertretungen) an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Rheinland-Pfalz herangetreten und haben um eine Einschätzung gebeten, ob entsprechende Angebote bedenkenlos verwendet werden können. Auf diese Anfragen geht der LfDI mit den nachfolgenden Ausführungen ein. Da in diesem Bereich fast täglich neue technische und rechtliche Entwicklungen zu verzeichnen sind, kann die folgende Darstellung nur eine Momentaufnahme sein. Bestimmte Bedenken treffen nur auf manche Anbieter zu. Teilweise unternehmen große Software-Anbieter auch Anstrengungen, um den Datenschutz zu verbessern; entsprechende Bemühungen begrüßt der LfDI. Es folgen Gründe, weswegen der Einsatz einer Reihe außereuropäischer Anwendungen auf Bedenken stößt:

1) **Europäisches Urteil zur Rechtsgrundlage**: Nach einem Urteil des Europäischen Gerichtshofs ("Schrems II") vom Juli 2020 ist es derzeit für Schulen kaum möglich, rechtssicher Anbieter zu nutzen, bei denen Daten in die USA oder andere Drittstaaten außerhalb der EU abfließen. Es steht ihnen für diese Datenübertragung faktisch keine Rechtsgrundlage zur Verfügung. Auch können die Schulen kaum ihrer nach der Datenschutz-Grundverordnung bestehenden Pflicht nachkommen, Eltern und Schülerinnen und Schüler zu informieren, was mit den erhobenen Daten passiert, denn aufgrund der Intransparenz einer Reihe von US-Anbietern können Lehrkräfte dies regelmäßig selbst nicht abschätzen.

2) **Intransparenz:** Viele Datenverarbeitungsprozesse insbesondere bei US-Anbietern sind intransparent. Es ist nicht immer klar, ob die Daten vom jeweiligen Anbieter auch für eigene Zwecke verwendet werden. Falls beispielsweise Inhalte von Videokonferenzen tatsächlich zur Kenntnis genommen, analysiert oder gespeichert werden, eröffnet dies ein Missbrauchspotenzial. Trotz der Bemühungen einiger Anbieter, hier etwa durch Verschlüsselung zu Verbesserungen zu gelangen, sind nicht alle Unklarheiten über die Verwendung der Daten – insbesondere der Nutzungsdaten - ausgeräumt. Diese Problematik betrifft nicht nur Hackerangriffe, sondern auch die Nutzung dieser Daten zur Bildung von Persönlichkeitsprofilen, die zum Nachteil der Betroffenen genutzt werden können.

3) **Digitale Souveränität:** Wer mit einem Programm chattet, videotelefoniert oder Dokumente verschickt, hinterlässt beim Anbieter in aller Regel verschiedene Nutzungsdaten – etwa IP-Adresse, Informationen über die Dauer und anderen Teilnehmenden eines Gesprächs, Standortdaten und Angaben über das jeweilige Endgerät. Dies gilt gerade auch für Anwendungen, die Daten in der Cloud ablegen. Die Konzentration auf marktbeherrschende außereuropäische Plattformen birgt das Risiko, sich bewusst oder unbewusst in technische Abhängigkeiten zu begeben, die die Möglichkeiten einschränken, in der digitalen Welt selbständig, selbstbestimmt und sicher agieren zu können. Die Möglichkeit, eigenständig entscheiden zu können, wie die festgelegten Grundsätze für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind, kann gefährdet sein. Dies erfordert Wahlfreiheit und vollständige Kontrolle über die eingesetzten Mittel und Verfahren bei der Verarbeitung von personenbezogenen Daten. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden. Diese vermeiden auch unerwünschte Lock-in-Effekte.

4) **Mangelnde Datenhoheit**: Werden Daten auch außerhalb der EU gespeichert, werten US-Sicherheitsbehörden sie möglicherweise aus und führen sie mit anderen zusammen. Es gibt eine „no fly list“, auf der die Namen von Personen stehen, denen aus Gründen der Terrorismusabwehr die Einreise in die USA verwehrt wird, ohne dass die Kriterien öffentlich bekannt sind, aufgrund derer man auf die Liste gelangt. Für EU-Bürgerinnen und Bürger gibt es keine Möglichkeit, ein US-Gericht anzurufen, um zu erfahren, ob und welche ihrer Daten durchleuchtet oder gespeichert wurden. Zwar haben manche US-Anbieter angekündigt und dies auch bereits umgesetzt, gegen US-Behörden juristisch vorzugehen, wenn diese auf die Daten von EU-Bürgerinnen und EU-Bürgern zugreifen oder zugreifen wollen; das bedeutet aber nicht, dass damit ein Zugriff verhindert werden kann.

5) **Verwendung für Werbezwecke**: Wer manche Produkte nutzt, muss befürchten, dass Nutzungsdaten, wie die User-ID zu Werbepartnern oder Tracking-Unternehmen gelangen. Auch wenn der konkrete Anbieter selbst keine Werbung schaltet, ist nicht ausgeschlossen, dass die Daten von Dritten dafür genutzt werden können. Bezogen auf Schulen würde dies bedeuten: Schülerinnen und Schüler wären unfreiwillig gezieltem und gegebenenfalls manipulativem Marketing ausgesetzt, nur weil sie ihrer Schulpflicht nachkommen und am Unterricht teilnehmen. Die Regelungen in den Schulordnungen untersagen aber, die Daten von Schülerinnen und Schülern für Werbezwecke zu verwenden.

6) **Datenschutz für Minderjährige**: Schülerinnen und Schüler sind häufig noch nicht volljährig: Ihre Daten müssen nach der europäischen Datenschutz-Grundverordnung besonders geschützt werden.

7) **Medienkompetenz**: Schülerinnen und Schüler sollen – so der Bildungsauftrag – eine digitale Selbständigkeit erlangen, also lernen, selbständig IT-Produkte zu bewerten, auszuwählen und die Hoheit über ihre Daten auszuüben. Manche US-Unternehmen versuchen über meist kostengünstige Schul-Lizenzen, Kinder und Jugendliche an die eigenen Produkte zu gewöhnen. Dem liegt offenbar die Überlegung zugrunde, dass später in beruflichem oder privatem Zusammenhang auf diese kommerziellen Produkte zurückgegriffen wird, mit denen man ja vertraut ist. Schulen können so zum Marktplatz werden, um Neukunden zu gewinnen. Indem Bildungseinrichtungen auf Open Source-Software und offene Standards setzen, regen sie digitale Selbständigkeit, Kreativität und Vielseitigkeit an.

8) **Auswirkungen auf die Meinungsvielfalt:** Einige internationale Digitalunternehmen versuchen den Nutzer oder die Nutzerin in ihr eigenes „Universum“ zu ziehen und dort festzuhalten. Man soll nur dort chatten, nur von dort Nachrichten beziehen und sich nur dort digital bewegen. Entsprechende Entwicklungen können zu Monopolstellungen führen. Sie bergen Gefahren für die freie Meinungsbildung. Dies kann die Wahrnehmung von Vielfalt beeinträchtigen, die in der demokratischen Gesellschaft essentiell ist.

9) **Unterschiedliche Datenschutz-Traditionen:** Viele außereuropäische Produkte sind zum Teil nicht datenschutzfreundlich programmiert. Ein Grund ist, dass eine entsprechende Tradition und Grundhaltung wie in der Europäischen Union nicht weltweit gegeben ist; der Datenschutz hat zum Beispiel in den USA nicht denselben Stellenwert wie in Europa. Mit der Datenschutz-Grundverordnung hat die EU ein einheitliches Datenschutzrecht geschaffen, das weltweit seinesgleichen sucht.

10) **Datenschutzbewusstsein**: Die fortschreitende Digitalisierung führt dazu, dass sich in nahezu allen Lebensbereichen datenschutzrechtliche Bezüge ergeben. Daher sollten Kinder und Jugendliche frühzeitig auf die Bedeutung einer selbstbestimmten Verarbeitung ihrer Daten in einer digitalisierten Welt vorbereitet werden. Hierzu zählt auch die Erfahrung, dass Datenschutzrechte nicht auf dem Altar der Funktionalität geopfert werden müssen, sondern Alternativen bestehen, die gleichermaßen eine datenschutzgerechte und funktionale Nutzung ermöglichen.