

04.03.2021

Antwort

der Landesregierung

auf die Kleine Anfrage 4912 vom 2. Februar 2021
der Abgeordneten Sigrid Beer und Matthi Bolte-Richter BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/12522

Riskantes Videokonferenztool von LOGINEO Messenger

Vorbemerkung der Kleinen Anfrage

Am 01.02.2021 berichtet die Süddeutsche Zeitung unter dem Titel „Riskante Konferenzen“, dass das Videokonferenztool von Logineo Messenger, das im Januar eingeführt worden ist, erhebliche Risiken für den Datenschutz aufweist. Demnach könnten sich schulfremde Personen einschalten, sofern sie den Einwahllink haben. Eine Überprüfung der Teilnehmenden vor Eintritt finde nicht statt. Der Hinweis des Schulministeriums, die Weitergabe des Links sei nicht rechtmäßig, ist keine adäquate Antwort auf eine Sicherheitslücke. Tatsächlich hat es Fälle bei der Benutzung auch anderer Videokonferenztools gegeben, wo schulfremde Personen in den virtuellen Raum eingedrungen sind, Lehrkräfte stummgeschaltet oder sogar pornografische Inhalte eingespielt haben. Das geschieht, wenn der Zugang und die Möglichkeit den Bildschirm zu teilen, nicht beschränkt wird. Dem Bericht zufolge wurden die Schulbehörden im Dezember darauf hingewiesen, dass beim Videokonferenztool von Logineo Messenger diese Risiken bestehen.

In der Schulmail zur Einführung des Videokonferenztools heißt es: „Bei der digitalen Kommunikation sind der Datenschutz und die Datensicherheit von Kindern und Jugendlichen sowie von Lehrkräften besonders wichtig.“ Es irritiert, dass trotz der Warnungen keine Vorsorge getroffen wurde und keine Warnungen seitens des Ministeriums nach den ersten Vorfällen erfolgt sind.

Die DPA meldet am 31.01.2021 unter der Überschrift „Schülerstreiche im Digitalunterricht: ‚Großes Potential für Unfug‘“, dass es wiederholt Fälle gegeben hat, wo Schülerinnen und Schüler Teile von Videokonferenzen mitgeschnitten und anschließend in sozialen Medien wie TikTok geteilt haben. Das verstößt eindeutig gegen die Persönlichkeitsrechte der betroffenen Schülerinnen und Schüler wie der Lehrkräfte. Schulministerin Gebauer wird zitiert mit den Worten: Mit schützenswerten persönlichen Daten darf kein Unfug getrieben werden. Persönlichkeitsrechte sind gerade bei Videokonferenzen zu beachten.“ Weiter heißt es in dem Beitrag: „Sie sei sich sicher, dass sich dabei alle ihrer Verantwortung bewusst seien.“ Das irritiert, denn es fragt sich, woher die Ministerin die Sicherheit nimmt, dass alle Schülerinnen und Schüler über die Persönlichkeitsrechte ausreichend informiert und sich ihrer Verantwortung bewusst sind.

Datum des Originals: 04.03.2021/Ausgegeben: 10.03.2021

Die WAZ berichtet am 01.02.2021, dass die Schulleitung eines Gymnasiums in Duisburg angeordnet hat, dass sich zukünftig alle ohne Ausnahme mit der Kamera bei Videokonferenzen einschalten müssen. Hier stellt sich die Frage, wie berechnigte Bedenken hinsichtlich der Gewährleistung von Persönlichkeitsrechten aus unterschiedlicher Perspektive grundsätzlich vereinbart werden können mit der Nutzung von Videotools.

Die Ministerin für Schule und Bildung hat die Kleine Anfrage 4912 mit Schreiben vom 4. März 2021 namens der Landesregierung beantwortet.

Vorbemerkung der Landesregierung

Die Landesregierung verfolgt seit Amtsantritt die Digitalisierung von Schulen als eines ihrer wichtigsten schulpolitischen Ziele. Die Bedeutung dieses Vorhabens wird gerade in der Corona-Pandemie deutlich, wenn Unterricht zeitweise auf Distanz erfolgt. Um Schulen dabei zu unterstützen, wurde die Weiterentwicklung der digitalen Anwendungen im Rahmen von LOGINEO NRW, die das Land Schulen zur kostenlosen Nutzung zur Verfügung stellt, stark beschleunigt. Inzwischen stehen neben dem Schulportal LOGINEO NRW auch das Lernmanagementsystem

LOGINEO NRW LMS und der LOGINEO NRW Messenger zur Verfügung. Dieser wurde am 21. Januar 2021 um eine Videokonferenzoption ergänzt. Damit wurde auch – berechtigten – Forderungen von Schulen entsprochen, da ein Videokonferenztool für den Distanzunterricht eine große Unterstützung darstellen kann.

Obwohl bei allen Anwendungen im Rahmen von LOGINEO NRW Sicherheit und Datenschutz zentrale Aspekte sind, ist anzumerken, dass bei digitalen Anwendungen durch technische Maßnahmen eine missbräuchliche Nutzung nicht vollständig ausgeschlossen werden kann. Dies gilt für die Produkte der LOGINEO-NRW-Familie ebenso wie für alle anderen Anbieter. Ergänzend zu den umfassenden technischen Schutzmaßnahmen sind daher vor allem pädagogische Maßnahmen erforderlich, wie sie etwa im Medienkompetenzrahmen NRW verankert sind.

1. Seit wann weiß das Schulministerium um die Sicherheitsbedenken und Risiken beim Videokonferenztool von Logineo Messenger?

Transparenz ist im Umgang mit möglichen Risiken sehr wichtig. Deshalb haben auch alle Nutzerinnen und Nutzer die Möglichkeit, Bedenken oder erkannte Risiken – auch direkt an das Ministerium für Schule und Bildung – zu melden. Diese Möglichkeit wird auch genutzt. Sämtliche potenzielle und tatsächliche Risiken und Bedenken, die uns seit dem Start des Videokonferenztools erreicht haben, werden umgehend analysiert, bewertet und entsprechende Maßnahmen werden ergriffen.

2. Waren diese Fragen in Bezug auf den Datenschutz und den Schutz der Persönlichkeitsrechte bei der Nutzung des Videokonferenztools Gegenstand der Bedenken und Fragen im Rahmen des Mitbestimmungsverfahrens im Ministerium für Schule und Bildung?

Nein.

3. Mit welchen Maßnahmen sollen die Sicherheitslücken geschlossen werden?

Durch den erhöhten Einsatz von Videokonferenztools im Unterricht ist es zuletzt deutschlandweit zu Störungen durch unberechtigte Personen gekommen („Zoom-Bombing“). Aus diesem Grund wurde umgehend mit der Umsetzung einer sogenannten Lobbyfunktion begonnen, also einem virtuellen Warteraum, die es Lehrkräften ermöglicht, Beitrittsanfragen zu prüfen und unberechtigte Personen von der Teilnahme auszuschließen. Diese steht seit dem 08. Februar 2021 zur Verfügung. Darüber hinaus wird derzeit unter anderem ein Update vorbereitet, das Anpassungen beim Rechte-Rollen-Konzept beinhaltet. Wie alle Anwendungen im Rahmen von LOGINEO NRW befindet sich auch der LOGINEO NRW Messenger mit der integrierten Videokonferenzoption in einem kontinuierlichen Monitoring durch die beauftragten Dienstleister. Die Anwendungen werden fortlaufend weiterentwickelt, selbstverständlich unter Berücksichtigung von Rückmeldungen von Nutzerinnen und Nutzern.

4. Wie wird gesichert, dass sich alle Nutzerinnen und Nutzer der Videotools ihrer Verantwortung hinsichtlich der Achtung der Persönlichkeitsrechte und des Datenschutzes bewusst sind?

Die Nutzerinnen und Nutzer spielen eine wichtige Rolle im Hinblick auf die Sicherheit der Systeme. Das Land Nordrhein-Westfalen verfolgt das Ziel, Schülerinnen und Schüler medienpädagogisch zu unterstützen. Hierfür hat das Ministerium für Schule und Bildung unter anderem zur Sensibilisierung und Entwicklung eines sicheren und verantwortungsvollen Umgangs mit Medien sowie zum Datenschutz und zur Informationssicherheit den Medienkompetenzrahmen NRW entwickelt (<https://medienkompetenzrahmen.nrw>).

Außerdem können Lehrkräfte auf der LOGINEO-NRW-Website auf Unterstützungsmaterialien zurückgreifen, wie zum Beispiel auf das Dokument „Wichtige Hinweise für die sichere Nutzung der Videokonferenzoption im LOGINEO NRW Messenger“, die einen sichereren Umgang mit dem Videokonferenztool erläutern (<https://www.logineo.schulministerium.nrw.de/LOGINEO-NRW/NEU-LOGINEO-NRW-Messenger/Messenger.html>).

5. Wie beurteilt die Landesregierung rechtlich eine Anordnung, dass die Kameras zwingend einzuschalten sind bei einer Teilnahme an Videokonferenzen im Distanzunterricht?

Die Verarbeitung von Audio- und Videodaten mit Personenbezug durch die Schule erfordert die Einwilligung der Betroffenen bzw. deren Erziehungsberechtigten, sofern Minderjährige das 16. Lebensjahr noch nicht vollendet haben.

Wirksame Einwilligungen bedürfen u.a. der Informiertheit der Betroffenen, d.h., dass letztere vor der beabsichtigten Verarbeitung ihrer personenbezogenen Daten hinreichend über die Umstände der Datenverarbeitung zu informieren sind. Dies bestätigen die Nutzerinnen und Nutzer bei LOGINEO-Produkten im Rahmen der Kontoaktivierung bei Erstanmeldung.

Eine Einwilligung bedarf nicht zwingend einer Schriftform. Sie kann auch durch eine sonstige eindeutig bestätigende Handlung erfolgen, mit der die betroffene Person in dem jeweiligen Kontext ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten unmissverständlich signalisiert (vgl. Art. 4 Nr. 11 DSGVO sowie Erwägungsgrund 32 DSGVO). Im Falle der Nutzung des von der Schule bereitgestellten Videokonferenzsystems kann somit auch das bloße Einschalten von Kamera und/oder Mikrofon (ggf. in Verbindung mit

der dazu erteilten Erlaubnis der jeweils Erziehungsberechtigten) als wirksame Einwilligung gewertet werden.

Als Einwilligung in die Verarbeitung der Audio- und Videodaten mit Personenbezug im Rahmen der Bereitstellung und Nutzung des Videokonferenzsystems der Schule wird das (ggf. durch die Erziehungsberechtigten erlaubte) Einschalten der Kamera bzw. des Mikrofons angesehen (vgl. Art 4 Nr. 11 DSGVO sowie Erwägungsgrund 32 DSGVO).

Die Einwilligung kann jederzeit, z. B. durch Ausschalten von Kamera oder Mikrophon, widerrufen werden.