Die Landesbeauftragte für den
Datenschutz Niedersachsen

FAQ Einsatz von Videokonferenzsystemen in Schulen (Mai 2021)

Aufgrund der aktuellen pandemischen Lage erfolgt der Schulunterricht verstärkt als Distanzunterricht. Hierzu greifen Schulen regelmäßig auf Videokonferenzsysteme (VKS) zurück. Hierbei handelt es sich um Softwareprogramme, mit denen mehrere Personen kommunizieren und sich dabei zugleich hören und sehen können. In diesem Kontext wird eine Vielzahl personenbezogener Daten verarbeitet. Die folgenden häufig gestellten Fragen und Antworten (FAQ) sollen den Schulen eine Hilfestellung bieten, was beim Einsatz von Videokonferenzsystemen aus datenschutzrechtlicher Sicht zu beachten ist.

1. **Dürfen Schulen VKS einsetzen und in diesem Zuge personenbezogene Daten verarbeiten?**

   Ja, die Verarbeitung personenbezogener Daten ist gemäß § 31 Absatz 5 Satz 2 i.V.m. § 31 Absatz 1 Nds. Schulgesetz (NSchG) zulässig. Demnach darf die Schule u.a. dann personenbezogene Daten von Schülerinnen und Schülern (SuS) sowie Lehrkräften mit Hilfe digitaler Lehr- und Lernmittel (z. B. VKS) verarbeiten, wenn dies zur Erfüllung des Bildungsauftrags der Schule erforderlich ist. Hierzu gehört zum Beispiel die Durchführung des Unterrichts. Diese Erforderlichkeit ist derzeit auf Grund des pandemiebedingten Ausfalls des Präsenzunterrichts gegeben. Dies bedeutet jedoch nicht, dass SuS sowie Lehrkräfte zur Durchführung von Videokonferenzen ohne Weiteres verpflichtet werden können (siehe Frage 3).
   Von § 31 Absatz 5 Satz2 i.V.m. § 31 Absatz 1 NSchG ist zudem nicht gedeckt, wenn Nutzungsbedingungen des Anbieters eines bestimmten VKS-Programms zugestimmt werden muss.

2. **Welche personenbezogenen Daten dürfen auf gesetzlicher Grundlage verarbeitet werden?**
   Verarbeitet werden dürfen insbesondere: Die IP-Adresse der Teilnehmerinnen und Teilnehmer, die Bild- und Tonübertragung der Teilnehmerinnen und Teilnehmer, geteilte Dateien sowie der Nachrichtenaustausch unter den Teilnehmerinnen und Teilnehmern während der Videokonferenz (Chats).

3. Kann der Einsatz von Videokonferenzen von der Schulleitung verpflichtend angeordnet werden?

a) gegenüber Lehrkräften?

Grundsätzlich ja, da die Dienststelle über ein sogenanntes „Direktionsrecht“ verfügt. Beamtinnen und Beamte haben eine Folgepflicht und müssen auf Weisung ihres/ihrer Vorgesetzten ein Videokonferenzsystem nutzen. Eine Verpflichtung setzt voraus, dass die Lehrkräfte Dienstgeräte haben und das schulische Internet nutzen können. Lehrkräfte können nicht verpflichtet werden, ihre private IT (Geräte, Internetverbindung) für die dienstliche Tätigkeit einzusetzen.

b) gegenüber Schülerinnen und Schülern?

Eine Verpflichtung der Schülerinnen und Schüler scheitert bereits dann, wenn keine Schulgeräte zur Verfügung gestellt werden oder die private Internetverbindung – sofern überhaupt vorhanden – genutzt werden müsste.
Daher ist der Einsatz privater Endgeräte und privater Internetzugänge nur auf freiwilliger Basis möglich.

4. Worauf muss bei Einholung einer Einwilligung geachtet werden?

Die Einwilligung muss informiert erfolgen, d.h., dem Betroffenen muss bekannt sein, zu welchem Zweck sie erteilt wird. Des Weiteren muss ein Hinweis auf die Widerrufsmöglichkeit enthalten sein und die Einwilligung muss freiwillig erfolgen.
Das heißt, Personen, die ihre Einwilligung nicht erteilen, dürfen keine Nachteile befürchten müssen (z. B. Ausschluss von Unterrichtsinhalten), wenn sie nicht einwilligen. Sofern keine Teilnahme an der Videokonferenz erfolgt, muss eine Alternative (z.B.: Bereitstellung von Unterrichtsmaterial auf anderem Wege z.B. elektronisch oder per Post) hierzu vorgehalten werden.

5. Ist das Aufheben der Stummschaltung durch die Lehrkraft ohne Hinweis bei einer VK erlaubt?

Nein, da das Aufheben der Stummschaltung ohne vorherigen Hinweis eine Verletzung des grundgesetzlich geschützten Rechts am eigenen Wort darstellt. Die SuS sollen bewusst darüber entscheiden können, wann sie zu hören sind und wann nicht.

6. Wer ist für den Betrieb von VKS datenschutzrechtlich verantwortlich?

Verantwortlich ist die Schule, vertreten durch die Schulleiterin bzw. den Schulleiter.

7. Welche weiteren datenschutzrechtlichen Pflichten hat die Schule?

Insbesondere sind folgende datenschutzrechtliche Pflichten zu beachten:

a) Eintrag in das Verzeichnis von Verarbeitungstätigkeiten der Schule (Art. 30 DS-GVO).

b) Information der Teilnehmerinnen und Teilnehmer, deren personenbezogene Daten durch das VKS verarbeitet werden, über die Verarbeitung der personenbezogenen Daten und die ihnen zustehenden Rechte (Art. 13, 14 DS-GVO).

c) Prüfung, ob eine Datenschutzfolgenabschätzung (Art. 35 DS-GVO) durchgeführt werden muss.

8. Wie können VKS betrieben werden?

VKS können entweder von der Schule selbst auf einem eigenen Speicherort (Server) oder von Dritten auf deren Servern, sogenannten Auftragsverarbeitern (AV), für die Schule betrieben werden. AV dürfen jedoch gemäß Art. 28 DS-GVO nur unter bestimmten Voraussetzungen eingebunden werden: Sie dürfen die personenbezogenen Daten, die sie durch den Betrieb des VKS erhalten, ausschließlich auf Weisung der Schule verarbeiten. Zudem muss die Schule als Verantwortliche den Dritten und sein Handeln jederzeit überprüfen können. Darüber hinaus muss eine Verarbeitung der Daten zu eigenen Zwecken durch den Dritten ausgeschlossen sein. Dies muss in einem Vertrag zwischen der Schule und dem Dritten festgehalten werden. Zudem ist darauf zu achten, dass der Dritte seine Server innerhalb der Europäischen Union betreibt und dass keine personenbezogenen Daten an weitere Dritte übermittelt werden.

9. Dürfen Erziehungsberechtigte an den Videokonferenzen teilnehmen?

Nein, es dürfen grundsätzlich weder Erziehungsberechtigte noch andere schulfremde Personen an Videokonferenzen explizit teilnehmen (Ausnahme: notwendige Schulbegleitungen). Natürlich ist es möglich, insbesondere jüngere Schülerinnen und Schülern beim Einrichten der Videokonferenz zu helfen, aber eine andauernde Teilnahme ist nicht zulässig, auch wenn aufgrund verschiedener, beengter Wohnverhältnisse ein Mithören u.U. nicht immer ausgeschlossen werden kann.

Nur wenn alle Beteiligten eine entsprechende Einwilligung erteilen würden, dürfen weitere Personen an einer Videokonferenz teilnehmen.

10. Können auch Konferenzen digital durchgeführt werden?

Klassenkonferenzen nach § 35 Abs. 2 Nr. 5 (Zeugniskonferenz) und § 61 NSchG (Ordnungsmaßnahmenkonferenz) sollen in Präsenz und können – etwa aus Infektionsschutzgründen – in digitaler Form durchgeführt werden; die Entscheidung hierzu obliegt der Schulleiterin bzw. dem Schulleiter.
Auch im Rahmen einer digitalen Klassenkonferenz sind die allgemeinen Grundsätze, wie z.B. der Grundsatz der Verschwiegenheit zu beachten.

11. Dürfen Videokonferenzen aufgezeichnet werden?

Für den Schulregelbetrieb ist die Aufzeichnung von VK nicht notwendig und daher nicht von § 31 Absatz 5 Satz 2 i.V.m. § 31 Absatz 1 NSchG gedeckt. Es bedarf daher im Falle einer Aufzeichnung der gesonderten Einwilligung der betroffenen Personen, da nur die Durchführung von Videotelefonaten (Übertragung in Echtzeit) von der Rechtsgrundlage des § 31 Absatz 5 Satz 2 i.V.m. § 31 Absatz 1 NSchG gedeckt ist. Die Freiwilligkeit der Einwilligung ist dabei sicherzustellen (**siehe Frage 4**). Zudem sind Regelungen zu Aufbewahrungs- und Löschfristen zu treffen.

12. Was kann getan werden, wenn heimlich gefertigte Unterrichtsmitschnitte veröffentlicht werden?

Das Veröffentlichen (und auch bereits das Aufzeichnen) heimlich gefertigter Unterrichtsmitschnitte ist verboten und kann strafrechtlich verfolgt werden. Die Schülerinnen und Schüler (und bei Minderjährigkeit die Erziehungsberechtigten) sollten schon im Vorfeld darauf hingewiesen werden, dass ein Mitschnitt, eine sonstige Speicherung der übermittelten Daten oder eine Weitergabe der Daten an Dritte nicht erlaubt ist. Es bietet sich an, diesen Hinweis in der Einwilligungserklärung aufzunehmen oder ein gesondertes Schreiben zu Verhaltensregeln im Distanzunterricht an die Erziehungsberechtigten und Schülerinnen und Schüler herauszugeben. Ein Beispiel für ein solches Schreiben finden Sie hier.
Alternativ kann die Schule das o.g. Verbot auch im Rahmen einer Nutzungsordnung für die Nutzung des Videokonferenzsystems vermerken.
Mögliche Maßnahmen bei Verstößen sind:

- Erzieherische Einwirkung (Erziehungsmittel und Ordnungsmaßnahmen gem. § 61 NSchG)
- Zivilrechtliche Unterlassungs- und Beseitigungsansprüche gegenüber Schülerinnen und Schülern bzw. Erziehungsberechtigten und dem Betreiber der Plattform, auf die hochgeladen wurde

- Meldung einer Datenschutzverletzung bei der Landesbeauftragten für den Datenschutz Niedersachen
- Je nach Schwere des Verstoßes kommt auch die Verwirklichung von Straftatbeständen wie z.B. § 201 Strafgesetzbuch in Betracht (siehe hierzu auch den Gem. RdErl. des MK, des MI und des MJ vom 01.06.2016 „Sicherheits- und Gewaltpräventionsmaßnahmen in Schulen in Zusammenarbeit mit Polizei und Staatsanwaltschaft“), ein Verstoß gegen §§ 22, 23, 33 Kunsturhebergesetz oder auch zivilrechtliche (Schadensersatz-) Ansprüche.

13. Sollte ich als Lehrkraft im Hinblick auf Hacker-Angriffe bestimmte Sicherheitsmaßnahmen ergreifen?

Lehrkräfte sollten technisch die Möglichkeit haben, eine Teilnahme an der Videokonferenz zuzulassen oder abzulehnen. Zudem sollten die Schülerinnen und Schüler darauf hingewiesen werden, dass sie die Zugangsdaten nicht weitergeben. Auch sollten die Lehrkräfte die Zugangsdaten regelmäßig erneuern. Schülerinnen und Schüler sollten auch insoweit sensibilisiert werden, dass sie die Videokonferenz verlassen, wenn sie etwas Ungewöhnliches bemerken, sich insbesondere fremde Personen unerwartet der Videokonferenz zuschalten und die Lehrkraft durch Fremdeinwirken von der Videokonferenz ausgeschlossen wurde.

14. Was ist bei Auswahl und Betrieb von VKS aus Sicht des technischen und organisatorischen Datenschutzes zu beachten?

Die Ergebnisse einer evtl. durchzuführenden Datenschutzfolgeabschätzung (siehe Frage 7 c)) hat maßgeblichen Einfluss auf die technischen und organisatorischen Anforderungen an die VKS-Lösung. Zudem ist das jeweils gewählte Betriebsmodell (siehe Frage 8) zu Grunde zu legen. In jedem Fall bedarf es einer individuellen Prüfung, um die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des jeweiligen Risikos für die Rechte und Freiheiten der Betroffenen (insb. SuS, Lehrkräfte) zu untersuchen. Dabei sind, der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung mit zu berücksichtigen. Auf der Grundlage dieser Prüfung sind die notwendigen technischen und organisatorischen Maßnahmen zu ermitteln, mit denen das Risiko durch die Datenverarbeitung auf ein vertretbares Maß minimiert werden muss, um damit ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 5, 24, 25, 32 DS-GVO).

Insbesondere sind daher die folgenden Eckpunkte zu beachten:

- Es muss mindestens eine sogenannte Transportverschlüsselung eingesetzt werden. Es wird jedoch empfohlen, nur VKS einzusetzen, die mit einer sogenannten Ende-zu-Ende-Verschlüsselung arbeiten.

- Das VKS sollte vorab so eingestellt werden können, dass SuS nicht die Möglichkeit haben, durch Veränderung der Einstellungen (z.B. Aufzeichnung der Videokonferenz, Aktvieren/Deaktivieren der Stummschaltung anderer Teilnehmer etc.) Datenschutzverstöße herbeizuführen. Die Steuerung sollte allein durch die Lehrkraft erfolgen.
- Die Lehrkraft muss die Rolle der Konferenzmoderation innehaben und sicherstellen, dass Personen, die unbefugt teilnehmen, erkannt und ausgeschlossen werden.
- Das VKS muss die Möglichkeit bieten, allen Teilnehmerinnen und Teilnehmern klare Rollen und damit einhergehende Befugnisse und Beschränkungen zuzuweisen.

Diese Eckpunkte sind nicht abschließend. Um methodisch korrekt und vollständig vorzugehen und das jeweils angemessene Schutzniveau auch tatsächlich zu erreichen, wird auf die detaillierteren Ausführungen im Dokument „Technische Eckpunkte für den Einsatz eines VK-Systems in Schulen“ hingewiesen. Dort werden weitere Anhaltspunkte aufgezeigt, die für die Auswahl von Produkten und Dienstleistern, für die Implementierung und für den Betrieb eines VKS beachtet werden müssen.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail an poststelle@lfd.niedersachsen.de schreiben