Staatliches Schulamt für den Landkreis Groß-Gerau
und den Main-Taunus-Kreis

HESSEN

Datenschutz (DS-GVO)

Information des Staatlichen Schulamtes

für Schulleitungen und Datenschutzbeauftrage (DSB)

Videokonferenzsysteme (VKS)

Besant / 30.10.2020

Recht | VKS | Risiko-einschätzung | Risiko-minimierung | SSA-Kontakt

Staatliches Schulamt für den Landkreis Groß-Gerau
und den Main-Taunus-Kreis

HESSEN

1.0 Rechtlicher Rahmen

1.1 Übersicht (VKS)

Videokonferenzsysteme (VKS)		
Notwendige Datenschutzmaßnahmen * DSB und Schulleitung	DS-GVO konform	Nicht DS-GVO konform
Risikoeinschätzung		
Software / Anbieter	Ja	ja
Hardware / Subunternehmer	ja	ja
Einwilligung		
Schülerinnen und Schüler	ja	ja
LK in der Schule	nein	nein
LK mit privaten Endgerät	ja	ja
Technische Maßnahmen		
Technische Funktionen einschränken	nein	ja (z.B. Schulträger)
Organisatorische Maßnahmen		
Datenschutzerklärung	Ja (Anbieter)	ja
TOP in Konferenz	nein	ja
Kenntnisnahme der Verantwortlichen	nein	ja
Benutzerordnung	ja	ja
Videokonferenz (VK)		
Unterricht	ja	ja
Klassen- und Schulkonferenzen	ja	nein
DS-Verantwortliche -> Einladende	ja	ja
Alle VK-Inhalte DS-GVO konform	ja	ja

Abkürzungen:

DS-GVO: Datenschutz-Grundverordnung
DSB: Datenschutzbeauftragte an Schulen (Frau/Mann)
VKS: Videokonferenzsystem
VK: Videokonferenz
On-Premises: Vor Ort / Lokal
AVV: Auftragsverarbeitungs-vereinbarung
AGB: Allgemeine Geschäfts-bedingungen

TOP: Tagesordnungspunkt
LK: Lehrkraft

Zum Einsatz von VKS an Schulen sind die Rahmen-bedingungen der Handreichung (VKS) zu beachten.

1. Recht

Recht

1.2 für Schulen

Datenschutz-Grundverordnung (DS-GVO)

Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG)

Hessisches Schulgesetz (HschG)

§ 83 Abs. 1, § 83 Abs. 3, § 83 Abs. 1 S. 2 und 3, § 83 Abs. 9 HSchG:

Verordnung zur Verarbeitung personenbezogener Daten in Schulen (DS-VO)

1.3 EuGH Urteil

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 16. Juli 2020 (Rechtssache C311/18) den Beschluss 2016/1250 der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) für unwirksam erklärt.

Zugleich hat der EuGH festgestellt, dass die Entscheidung 2010/87/EG der Kommission über Standardvertragsklauseln (Standard Contractual Clauses - SCC) grundsätzlich weiterhin gültig ist.

Staatliches Schulamt für den Landkreis Groß-Gerau
und den Main-Taunus-Kreis

HESSEN

1.4 Videokonferenzsysteme (VKS) - Duldung

Während der Corona-Pandemie **duldet** der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) übergangsweise den Einsatz von VKS in Schulen auf der Grundlage von Art. 6 Abs. 1 Buchst. d) und e) der Datenschutz-Grundverordnung (DS-GVO). Die Duldung gilt für **alle VKS**, auch solche deren Datenschutzkonformität nicht eingeschätzt werden kann. Der Ausnahmefall gilt bis zum 31.07.2021.

Ein VKS ist ein Medium für den **Distanzunterricht**. Der konkrete Einsatz eines VKS ist auf das Notwendige zu beschränken und mit weiteren digitalen und analogen Werkzeugen zu verknüpfen.

Die **Duldung** setzt voraus, dass

a) jede Schule im **konkreten Einzelfall** das gewählte VKS (Anbieter) prüft und ggf. **technische und organisatorische Maßnahmen** zur Sicherstellung der **Datenschutzkonformität** umsetzt.
b) soweit der zuständige Schulträger oder das Land Hessen datenschutzkonforme VKS als "On-Premises" Lösung anbieten, diese einzusetzen (Landesnetzwerk oder Kommunales Netzwerk) sind.
c) die Nutzung **eines VKS** für **pädagogische Zwecke** (Unterricht) erfolgt. Der Einsatz in der Schulverwaltung, z.B. in Form von Klassen- oder **Schulkonferenzen**, ist für **nicht datenschutzkonforme VKS**, oder für VKS deren Konformität nicht geprüft oder beurteilt werden kann, **ausgeschlossen**.
d) der Unterricht via VK, die datenschutzrechtlichen Bedingungen (DS-GVO) einhält und ein mögliches **Datenschutzrisiko** durch organisatorische Maßnahmen **minimiert**. Die **Verantwortlichen** regeln die Einhaltung der Rahmenbedingungen.

1. Recht

2.0 VKS

2.1 VKS - Auftragsverarbeitungsvereinbarung

Das VKS sollte nach Erkenntnis aller vorliegenden Unterlagen DS-GVO konform sein. Die DS-GVO Konformität ergibt sich in der Regel aus dem Vertrag, der Datenschutzerklärung, den AGB und der **Auftragsverarbeitungs-vereinbarung** (AVV) zwischen dem Auftraggeber (Schule) und dem Auftragsverarbeiter (Anbieter des VKS).

Die Auftragsverarbeitungsvereinbarung (AVV) **verpflichtet die Anbieter zur Mitwirkung der Einhaltung des Datenschutzes**, insbesondere hinsichtlich der **physischen Datenverarbeitung**. Die Bestätigung der DS-GVO Konformität muss auch für **alle Subunternehmer des Anbieters** ersichtlich sein. Die AVV darf Regelungen aus dem DS-GVO nicht ausschließen.

Die AVV (DS-GVO, Art. 28 Abs. 3) legt die Anwendungsbereiche, die Verantwortlichkeiten, die Pflichten des Auftraggebers und des Auftragnehmers, den Umgang mit Anfragen von betroffenen Personen, die Nachweismöglichkeiten (z.B. Verhaltensregeln) und Zertifikate sowie die Haftung und den Schadensersatz fest. Insbesondere müssen **alle weiteren Subunternehmer verbindlich** aufgelistet werden.

Die Anlagen verdeutlichen Gegenstand und Dauer der Verarbeitung, weisungsberechtigte Personen und Datenschutzbeauftragte, Unterauftragnehmer sowie technische und organisatorische Maßnahmen nach Art. 32 DSGVO (vgl. auch § 3 Abs. 2)

Das **Land Hessen** hat einen Muster **AVV-Vertrag für seine Dienststellen**, der Grundlage für Auftrags-verarbeitungsvereinbarungen ist. Bei Fragen können Sie sich gerne an das Staatliche Schulamt wenden.

Staatliches Schulamt für den Landkreis Groß-Gerau
und den Main-Taunus-Kreis

HESSEN

2.2 VKS – Verantwortliche

Die Datenschutz-Grundverordnung (DS-GVO) schützt personenbezogene Daten, also alle Informationen, die einer Person zuzuordnen sind oder **eine Person eindeutig identifizierbar** machen. Dies sind Daten wie z.B. Name, Adresse, IP-Adresse, Bilder, Foto und Videomitschnitt.

Verantwortlich für den Schutz der Daten ist derjenige, der personenbezogene Daten verwendet, speichert, sortiert oder löscht.

Bei der Anwendung von VKS werden **alle Einladende** im Sinne des Datenschutzes zu „**Verantwortlichen**“ . Dies sind z.B. Lehrkräfte. Verantwortliche bleiben auch dann verantwortlich, wenn **diese sich Leistungen eines Dritten,** also eines **VKS Anbieters** bedienen.

Im Umgang mit VKS gilt, dass **keine Daten aufgezeichnet** oder **gespeichert** werden dürfen. Im Falle einer Zwischenablage muss das systematische, regelmäßige **Löschung aller Daten** sichergestellt sein. Für alle gespeicherten Daten müssen **Löschfristen** durch den Verantwortlichen definiert sein. Die Einhaltung dieser sollte automatisch geschehen. Falls dies nicht geschieht, haben Betroffene das **Recht auf die vollständige Auskunft**, und daraus folgend das Recht auf die Korrektur, die Löschung und die Einschränkung der Verarbeitung ihre Daten.

Anlage:
Einwilligungen
für SuS

2.3 VKS - Einwilligung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn die/der Einzelne die Nutzung ihrer/seiner Daten eingewilligt hat. Die Herstellung der Verbindung zu einem VKS durch die Teilnehmenden kann im einfachsten Fall als Einwilligung gelten. Dabei ist zunächst abzuwägen, ob die Verarbeitung die Rechte der Betroffenen verletzt.

Spätestens **wenn eine betroffene Person widerspricht, muss die Verarbeitung sofort beendet werden**. Der Wunsch von Betroffenen hat stets Vorrang. Deswegen sind Regelungen im Vorfeld der Nutzung von VKS notwendig. **Einwilligungen** sollen nicht generalisiert über alle Ausnahmen der DS-GVO gegeben werden sondern sind fall- und anwendungsbezogen.

Die Teilnahme an einer Videokonferenz (Unterricht) ist für **Schülerinnen und Schüler** grundsätzlich freiwillig und bedarf der **schriftlichen Einwilligung** aller an der VK Beteiligten bzw. ihrer Erziehungsberechtigten.

Für die Teilnahme von **Lehrkräften an den Videokonferenzen** zur **Übertragung des Präsenzunterrichts** an nicht präsente Schülerinnen und Schüler **bedarf es keiner Einwilligung durch die einzelne Lehrkraft.** In dem Fall, in dem die **Lehrkraft von zuhause** (mit dem privaten Endgerät) aus den Unterricht per VKS gestaltet, ist dagegen die **Einwilligung erforderlich**, weil von der Datenverarbeitung das private, häusliche Umfeld betroffen ist.

In die Einwilligung für **Lehrkräfte (Personal) empfehlen** wir die **Zusicherung der Schulleitung** zu integrieren, dass **geheime Zuschaltungen** durch Dritte über technische oder organisatorische Maßnahmen ausgeschlossen sind.

Staatliches Schulamt für den Landkreis Groß-Gerau
und den Main-Taunus-Kreis

HESSEN

Anlage:
Datenschutz-
erklärung

2.5 VKS - Datenschutzerklärung

Die Datenschutzerklärung wird in der Regel durch den **Anbieter der Anwendung** zur Verfügung gestellt. Diese muss DS-GVO konform sein. Die **Verantwortlichen** der Schule (Schulleitung und Datenschutzbeauftragte) werden bei den Kontaktdaten eingetragen.

Die Datenschutzerklärung muss den **Teilnehmenden vor** der **Benutzung** eines **VKS** vorliegen. Darin wird erklärt welche Daten wie verarbeitet werden und auf welcher Legitimation dies beruht.

Grundsätzlich gilt das Prinzip der **Datensparsamkeit** in der Verarbeitung. **DS-GVO konform ist nur die Verarbeitung der Metadaten, die im Rahmen der Gesetze und der Betriebssicherheit zeitweise gespeichert werden dürfen.**

In einer Datenschutzerklärung müssen Art, Umfang und Zweck der Datenverarbeitung sowie die etwaige Übermittlung in Drittländer, Informationen über die die Verwendung von Cookies (Zugang über eine Internetseite) sowie eine Belehrung über die **anonymisierte Nutzung der Daten** beschrieben sein.

Zusätzlich muss über bestehende **Widerrufs- und Auskunftsrechte** und die Möglichkeiten deren Ausübung belehrt werden.

2.6 VKS - Benutzerordnung

Die DS-GVO gibt vor, dass „**Verantwortliche“ Maßnahmen** ergreifen müssen, um die anfallenden Daten zu schützen. Die **Benutzerordnung** dient der Festlegung von organisatorischen Maßnahmen und soll möglichen **Datenschutzverletzung** vorbeugen. Diese wird durch die **Schule** erstellt und von den Teilnehmenden zur **Kenntnis** genommen.

In die Benutzerordnung gehören verbindliche Verhaltensregeln für alle Anwender wie z.B.:

- Die **Speicherung von Daten** jeglicher Art bei der Nutzung einer VKS sind **ausgeschlossen**. Die/der Verantwortliche stellt den **datensparsamen Verlauf** einer **VK** sicher und löscht (z.B. eingestellte Unterlagen) **alle Inhalte** vor dem Schließen des virtuellen Raums.
- Der Hinweis, dass jede Art des **Aufzeichnens, Filmens oder Mitschneidens verboten ist**. Eine nicht erlaubte Aufzeichnung kann den **Straftatbestand** des § 201 Strafgesetzbuch erfüllen und schulische Ordnungsmaßnahmen nach sich ziehen.
- Die Beachtung der **Regeln** im Umgang mit dem **Urheberrecht**, den **Persönlichkeitsrechten** sowie der Einhaltung des **Datenschutzes ….**
- Regeln für den virtuellen Klassenraum. Wichtig ist, dass die/der Verantwortliche den Raum als erster öffnet und als letzter verlässt, sowie die Anwesenheit im virtuellen Raum sicher kontrolliert und dokumentiert (z.B. Klassenbuch).

Die Regeln können schulspezifisch erweitert und vor der Verabschiedung im Rahmen einer Konferenz abgestimmt werden. Die Benutzerordnung ist mit den DSB der Schule abzustimmen. Bei Fragen können Sie sich gerne an das Staatliche Schulamt wenden.

3.0 Risiko

3.1 Risiko - Einschätzung

Vor der Entscheidung für ein VKS in Schulen muss eine **Risikoeinschätzung** erfolgen. Die/der Datenschutzbeauftragte (DSB) der Schule ermittelt dazu das grundsätzliche Risiko.

- Wird **kein Datenschutzrisiko** auf Grundlage der notwendigen Unterlagen ermittelt, dokumentiert dies die/der DSB der Schule. Im Anschluss kann die Schule das VKS beschaffen.
- Wird **ein Datenschutzrisiko** ermittelt, dann müssen **geeignete Maßnahmen zur Risikominimierung** durch die Schule getroffen werden. Bei einem festgestellten **erheblichen und hohen Risiko** stimmt die Schule geeignete Maßnahmen mit dem **Staatlichen Schulamt** ab.

Im Rahmen der Beschaffung einer VKS werden neben den Vertragsunterlagen, die AGB, die Datenschutz-erklärung und die Auftragsverarbeitungsvereinbarung des Anbieters **zum Stichtag (Kauf)** aufbewahrt.

Anbieter passen z.B. die Datenschutzerklärung regelmäßig an. Eine Anpassung der o.g. Vereinbarungen nach dem o.g. Stichtag wird durch die Schule überwacht und führt zu einer neuen datenschutzrechtlichen Einschätzung durch die/den DSB der Schule. Die **vertragliche Bindung** ist nach einer Änderung des Risikos ggf. neu zu prüfen.

Wenn die Schule noch **keine** Beauftragte für den Datenschutz (DSB) hat, ist der **Datenschutzbeauftragte für den Schulamtsbereich des Staatlichen Schulamtes** mit in die Risikoeinschätzung einzubinden. Bei Fragen können Sie sich gerne an das Staatliche Schulamt wenden.

3.2 Risiko - Kriterien

Die Liste zeigt als besonders riskant eingestufte Kriterien. Wenn **mindestens eines** dieser Kriterien gegeben ist, liegen **Datenschutzrisiken** vor. Eine Risikominimierung muss dann umgesetzt werden.
(Datenschutzkonferenz des Bundes und der Länder)

Risiko erkennbar:		
0	Kein Risiko erkennbar.	
1	Daten werden im großem Umfang verarbeitet. (Anzahl der Betroffenen, Menge der Daten)	
2	Einsatz neuer Technologien oder biometrischer Verfahren.	
3	Systematische Überwachung von Personen.	
4	Bewerten oder Einstufung (Scoring /Profiling) von Personen und ihrer Verhältnisse.	
5	Datentransfer in Länder außerhalb der EU.	
6	Automatische Entscheidungsfindungen, die zu rechtlichen Folgen für die Betroffenen führen.	
7	Vertrauliche und sensible Daten. (besondere personenbezogene Daten aus Art. 9 DSGVO)	
8	Zusammenführen/ abgleichen von Daten die durch unterschiedliche Prozesse gewonnen werden.	
9	Daten Schutzbedürftiger (Kinder), geschäftsunfähiger oder beschränkt geschäftsfähiger Betroffener.	
10	Die Datenverarbeitung hindert Betroffene an der Rechtsausübung. Abtretung der Eigentumsrechte.	

Staatliches Schulamt für den Landkreis Groß-Gerau
und den Main-Taunus-Kreis

HESSEN

3.3 Risiko - Bewertung

Die Liste zeigt die Einstufung von Risiken. Im schulischen Bereich bewegen wir uns in der Regel im Bereich 1. und 2. Risikobereich (Bußgeld bei Verletzung möglich).
Risikoeinstufung: 1=gering / „tolerabel“ , 2=mittel / „erheblich“, 3= hoch / „besonders bedeutsam“

Einschränkung der Persönlichkeit:		
0	Ist für Betroffene nicht vorhanden.	
1	Ist für Betroffene als **tolerabel** einzustufen. Ein möglicher Datenmissbrauch hätte nur geringfügige wirtschaftliche/gesellschaftspolitische Auswirkungen. (Nicht zur Veröffentlichung bestimmte Daten, Geringfügige Schäden bei Veröffentlichung/Verfälschung: z.B.: Kontaktdaten, Verteilerlisten in E-Mails)	
2	Ist für Betroffene als **erheblich** einzustufen. Ein möglicher Datenmissbrauch hätte erhebliche wirtschaftliche/gesellschaftspolitische Auswirkungen für Betroffene. (Beeinträchtigung der persönlichen Unversehrtheit, sensible Daten, hohe Folgeschäden bei Veröffentlichung/Verfälschung: z.B. Finanzdaten, Beurteilungen, Gesundheitsdaten, Personaldaten)	
3	Wäre für Betroffene als **besonders bedeutsam** und als nicht tolerabel einzustufen. Ein möglicher Datenmissbrauch bedeutet für Betroffene den wirtschaftlichen/gesellschaftspolitischen Ruin oder beeinträchtigt die persönliche Unversehrtheit gravierend. (Hochsensible Daten , Veröffentlichung/Verfälschung verletzt Persönlichkeitsrechte, verursacht Schaden an Leib und Leben oder Ansehender Betroffenen, Erwägungsgründe wie z.B. Schutzprogramme)	

3.4 Risikominimierung

Wer Daten verarbeiten will, ist verpflichtet, im Verhältnis zum Risiko nach dem Stand der Technik angemessene Maßnahmen zum Schutz der Daten zu ergreifen, diese regelmäßig, bei Bedarf sogar unverzüglich zu überprüfen und regelmäßig zu aktualisieren.

In der Regel handelt es sich um eine Kombination aus

- **organisatorischen Maßnahmen** (z. B. Datenschutzschulung, **interne Regelungen** zum Datenschutz, Notfallkonzept). Dazu ist der **DSB der Schule** einzubinden.

und

- **technischen Maßnahmen** (z. B. Einsatz von Firewall und Virenscanner, Verschlüsselung von Daten, Eingrenzung von Möglichkeiten in der Benutzerführung die ein Risiko bedeuten). Wenn Rechner oder Lizenzen des Schulträgers verwendet werden, ist der **DSB des Schulträgers** einzubinden, um technische Maßnahmen zu prüfen.

Zu dokumentieren sind:

- die Durchführung einer **Risikoanalyse** auf Grundlage von geeigneten Unterlagen (Datenschutzerklärung, Verträge, AGB, bereits vorhandener Einschätzungen des Anbieters und deren Subunternehmer,….)
- das **Ergebnis** (geringes, mittleres, hohes Risiko) und die daraus abzuleitenden Maßnahmen.

4. Risikominimierung

4.1 Kein Datenschutzrisiko – So soll es sein!

- Die Teilnahme an einer Videokonferenz bedarf grundsätzlich des schriftlichen **Einverständnisses** aller Beteiligten.
- In der **Benutzerordnung** wird für die Teilnehmenden eines VKS auf den **datenschutzkonformen Umgang** mit den **Inhalten** hingewiesen. Dies beinhaltet z.B. den Umgang mit dem Urheberrecht, dem Verbot von Aufnahmen und Mitschnitten sowie das Einhalten der Persönlichkeitsrechte. Hierin werden die Verhaltensregeln für die Anwendung des VKS verbindlich definiert. Die Benutzerordnung ist mit der/dem DSB der Schule abzustimmen.
- Die Anwendung eines VKS birgt immer datenschutzrechtliche Risiken, die sich aus den Möglichkeiten der Bedienung eines VKS ergeben. Deshalb sollte pro **Schule nur ein VKS** verbindlich eingeführt werden. Alle Lehrkräfte einer Schule müssen durch Information und **Schulung** auf den Einsatz der VKS vorbereitet werden.
- Benutzte **Konferenzräume** eines VKS sollten nach der Beendigung der VK gelöscht werden, da es vorkommt, dass Verknüpfung mit Teilnehmenden bestehen bleiben, ohne als Teilnehmer zu erscheinen.
- Für **Dienstversammlungen**, die dem Schulverwaltungsbereich zuzuordnen sind (Schul-, Klassen-, Notenkonferenzen u.a.) gilt, dass, soweit ein datenschutzkonformes System zur Verfügung steht (also z.B. das vom Schulträger gehostete BBB), derartige Konferenzen virtuell darüber laufen können. Die technische Trennung des pädagogischen Bereiches vom Schulverwaltungsbereich kann ggf. über die Nutzung verschiedener Instanzen sichergestellt werden. Der **Datenschutz** ist innerhalb der VK einzuhalten. Themen wie z.B. Personal, Finanzen, Gesundheit und Beurteilungen sind von der VK ausgeschlossen.

4.2 Datenschutzrisiko vorhanden- Risikominimierung notwendig!!

Die Nutzung eines **nicht DS-GVO konformen VKS** ist nur für **pädagogische Zwecke** (Unterricht) erlaubt und gilt grundsätzlich nur vorübergehend, bis längstens zum Ende der Übergangsfrist zum 31.07.2021. Der Einsatz in der **Schulverwaltung**, z.B. in Form von Klassen- oder Schulkonferenzen, ist für nicht datenschutzkonforme VKS, oder für VKS deren Datenschutzkonformität nicht geprüft oder beurteilt werden kann, **ausgeschlossen**.

- Alle Verantwortliche (z.B. Lehrkräfte) sowie alle Teilnehmende sind bei einem vorliegenden Datenschutzrisiko nachweisbar auf den richtigen Umgang (Beachtung der Rechte, wie Datenschutz, Rechte der Betroffenen wie z.B. Urheberschutz, ….) mit dem VKS hinzuweisen.
- Die Schulleitung und die/der DSB der Schule informieren alle Verantwortlichen (Einladende) eines VKS über ein mögliches datenschutzrechtliches Risiko und den festgelegten Maßnahmenplan für die Benutzung. Dies wird als TOP in schulischen Konferenzen realisiert.
- Alle Teilnehmende am VKS müssen über die Maßnahmen eines **datenschutzgerechten** und **datensparsamen Handelns** im Rahmen der VK durch die „Verantwortlichen“ in Kenntnis gesetzt werden. Die Maßnahmen zum Umgang mit dem vorhandenen Datenschutzrisiko werden in der **Benutzerordnung** festgelegt und mit den **Teilnehmenden** besprochen.
- Die „Verantwortlichen“ gestalten die Inhalte und den Ablauf bei Nutzung einer VKS auf Grundlage der Kenntnis des bestehenden Datenschutzrisikos und der beschlossenen Maßnahmen zur Risikominimierung.

Risiko-minimierung

SSA-Kontakt

Staatliches Schulamt für den Landkreis Groß-Gerau
und den Main-Taunus-Kreis

HESSEN

6.0 Ansprechpartner

6.1 Datenschutz, Risikoeinschätzungen, Datenfälle

Datenschutzbeauftragter
für den Aufsichtsbereich

Gernot Besant
Tel.: +49 6142 5500 328
Gernot.Besant@kultus.hessen.de

Verwaltungsfachliche Generalistin
für den Aufsichtsbereich

Laia Lankenau
Tel.: +49 6142 5500 419
Laia.Lankenau@kultus.hessen.de

SSA-Kontakt