Landtag von Baden-Württemberg **Drucksache 16 / 4140**

16. Wahlperiode **23. 05. 2018**

Kleine Anfrage

der Abg. Klaus Hoher und Dr. Timm Kern FDP/DVP

und

Antwort

des Ministeriums für Kultus, Jugend und Sport

Auskunft über die „Schutzranzen“-App

Kleine Anfrage

Wir fragen die Landesregierung:

1. Inwieweit ist ihr die „Schutzranzen“-App (Website siehe: *schutzrantzen.com*) bekannt?

2. In welcher Weise hat sich die Landesregierung angesichts der öffentlichen Kritik von mehreren Datenschutzbeauftragten, Pädagogik- und Kinderhilfe-Verbänden sowie einer Online-Petition zum Thema mit der datenschutzrechtlichen Zulässigkeit der App befasst?

3. Inwieweit sieht die Landesregierung es als rechtmäßig an, dass eine dauerhafte Überwachung von Kindern, durch die Eltern, mit einer App ermöglicht wird?

4. Inwieweit hat das Kultusministerium den Schulen eine Handreichung zur Verwendung entsprechender Apps zur Verfügung gestellt?

5. Ist ihrer Kenntnis nach die Anonymität der im Rahmen dieser App an amerikanische Server übermittelten Standortdaten gewährleistet?

6. Wie bewertet sie bei einschlägigen Apps grundsätzlich die Verhältnismäßigkeit zwischen individuellem Datenschutz und Verkehrssicherheit?

7. Inwieweit empfiehlt die Landesregierung selbst die Nutzung von genannten Apps durch Schüler und Lehrer?

8. Sollten ihrer Auffassung nach auf satellitengestützten Standortdaten basierende Programme und Apps, welche dazu dienen, autonom fahrende Autos weiterzuentwickeln, zugelassen werden, auch wenn diese Technologien durch datensparsamere Sensorik ersetzt werden können?

Eingegangen: 23. 05. 2018 / Ausgegeben: 05. 07. 2018

9. Wie bewertet sie die Aussage des App-Anbieters, die betroffenen Schulkinder könnten in den Einstellungen der App selbst darüber entscheiden, wann sie der Überwachungen unterliegen bzw. wann nicht, mit Blick auf die Mündigkeit und das Problembewusstsein insbesondere jüngerer Schulkinder?

23. 05. 2018

Hoher, Dr. Timm Kern FDP/DVP

Begründung

Die „Schutzranzen"-App der Firma Coodriver verfolgt das Ziel, Kinder im Straßenverkehr zu schützen, indem Autofahrer gewarnt werden. Dieser Warnungsprozess wird durch eine App durchgeführt, welche dem Autofahrer zwar keinen genauen Standort des Kindes übermittelt, aber einen Sektor von ca. 150 Metern, in welchen sich der Schüler befindet, bekanntgibt. Auch die Eltern haben Zugriff auf diese App und bekommen Meldungen, wenn das Kind zum Beispiel in der Schule oder zuhause angekommen ist. Mit dieser Kleinen Anfrage soll die Einschätzung der App durch die Landesregierung erfragt werden.

Antwort

Mit Schreiben vom 18. Juni 2018 Nr. 13-/3856/196 beantwortet das Ministerium für Kultus, Jugend und Sport im Einvernehmen mit dem Ministerium für Inneres, Digitalisierung und Migration und dem Ministerium für Verkehr die Kleine Anfrage wie folgt:

Wir fragen die Landesregierung:

1. Inwieweit ist ihr die „Schutzranzen"-App (Website siehe: schutzrantzen.com) bekannt?

Dem Kultusministerium ist das Projekt „Schutzranzen" bekannt. Bereits vor geraumer Zeit hat sich der Hersteller der Software an das Kultusministerium gewandt und um Unterstützung bei der Einführung seines Produkts gebeten. Das Projekt Schutzranzen wurde bislang weder von einer Schule noch von der Kultusverwaltung betrieben. Das Kultusministerium erhielt diesbezügliche Anfragen im Zusammenhang mit Überlegungen der Stadt Ludwigsburg, das Projekt einzuführen.

2. In welcher Weise hat sich die Landesregierung angesichts der öffentlichen Kritik von mehreren Datenschutzbeauftragten, Pädagogik- und Kinderhilfe-Verbänden sowie einer Online-Petition zum Thema mit der datenschutzrechtlichen Zulässigkeit der App befasst?

Nachdem es sich bei der geplanten Einführung der App in Ludwigsburg um kein schulisches Projekt handelt, bestand für das Kultusministerium kein Anlass, datenschutzrechtliche Fragestellungen abschließend zu prüfen. Aus datenschutzrechtlicher Sicht ist dort nicht die Schule oder eine andere Einrichtung der Kultusverwaltung die sogenannte datenschutzrechtlich verantwortliche Stelle im Sinne der Datenschutzgrundverordnung. Aus den auf der Homepage von „Schutzranzen" verfügbaren Informationen ist im Übrigen eine abschließende datenschutzrechtliche Bewertung nicht möglich, da die Angaben unvollständig und an vielen Stellen unklar sind.

Nach Kenntnis des Kultusministeriums hat die Stadt Ludwigsburg den Landesbeauftragten für den Datenschutz und die Informationsfreiheit um eine datenschutzrechtliche Bewertung gebeten.

3. Inwieweit sieht die Landesregierung es als rechtmäßig an, dass eine dauerhafte Überwachung von Kindern, durch die Eltern, mit einer App ermöglicht wird?

Das Kultusministerium sieht kein Erfordernis für eine dauerhafte Überwachung von Kindern. Unabhängig von der datenschutzrechtlichen Zulässigkeit sieht das Kultusministerium bereits aus Gründen der Wettbewerbsneutralität keine Unterstützungsmöglichkeit derartiger Apps und hat deshalb die Nutzung solcher Apps weder empfohlen noch in irgendeiner Form beworben.

4. Inwieweit hat das Kultusministerium den Schulen eine Handreichung zur Verwendung entsprechender Apps zur Verfügung gestellt?

Das Kultusministerium hat im „Infodienst Schulleitung 268/September 2017“ Hinweise zum Datenschutz bei mobilen Endgeräten gegeben. Darin wurde auch auf einen Leitfaden zur Auswahl datenschutzkonformer Apps hingewiesen (s. *Anlage*). An der Erstellung der Dokumente zum Datenschutz war der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg beteiligt. Im Übrigen wird auf die Beantwortung der Frage 3 verwiesen.

5. Ist ihrer Kenntnis nach die Anonymität der im Rahmen dieser App an amerikanische Server übermittelten Standortdaten gewährleistet?

Dem Kultusministerium liegen keine Informationen über die technischen Sicherheitsmaßnahmen dieser App vor, sodass eine Bewertung nicht vorgenommen werden kann.

6. Wie bewertet sie bei einschlägigen Apps grundsätzlich die Verhältnismäßigkeit zwischen individuellem Datenschutz und Verkehrssicherheit?

Das Kultusministerium sieht keine Erforderlichkeit für eine dauerhafte Überwachung von Kindern. Eine abschließende datenschutzrechtliche Bewertung der speziellen Schutzranzen-App ist nicht möglich, da die Angaben auf der Homepage des Anbieters unvollständig und an vielen Stellen unklar sind. Die Verkehrssicherheit besitzt in Baden-Württemberg einen hohen Stellenwert. Beispielsweise werden folgende schulische Maßnahmen in Kooperation mit dem Innenministerium umgesetzt. Neben Schulweg- und Schulbustraining durch die Polizei finden an den Schulen Verkehrssicherheitstage, Radhelmkampagnen und Fahrradaktionstage statt. Darüber hinaus werden jährlich etwa 100.000 Viertklässler in der Radfahrausbildung im sicheren Umgang mit dem Fahrrad im Straßenverkehr geschult. Seit dem Schuljahr 2011/2012 sind die Schulen durch den Erlass „Sicherer Schulweg“ verpflichtet, gemeinsam mit den Kommunen Geh- und Radschulwegpläne zu erstellen, die den datenschutzrechtlichen Anforderungen entsprechen.

Zur Bewertung der Verbesserung der Verkehrssicherheit durch Apps sowie deren Datenschutzeinstellungen liegen dem Verkehrsministerium keine Erkenntnisse vor.

Die Landesregierung legt in ihrem Engagement für mehr Verkehrssicherheit ihren Fokus auf die Umsetzung der zahlreichen Maßnahmen des Verkehrssicherheitskonzepts der Landesregierung *(https://vm.baden-wuerttemberg.de/fileadmin/redaktion/m-mvi/intern/Dateien/PDF/Verkehrssicherheitskonzept_BW_2014.pdf)*.

7. Inwieweit empfiehlt die Landesregierung selbst die Nutzung von genannten Apps durch Schüler und Lehrer?

Das Kultusministerium sieht insbesondere unter pädagogischen Gesichtspunkten eine Förderung der Smartphone-Nutzung im Grundschulalter kritisch. Präventionsmaßnahmen in den Schulen und Präventionsangebote der Polizei für die richtige Nutzung von Handys und deren Gefahren werden in der Regel erst in den weiterführenden Schulen (ab Klasse 5) durchgeführt.

Ein Schwerpunkt der Schulwegsicherheit muss auf einem intensiven Schulwegtraining liegen, bei dem die Kinder lernen, aufmerksam im Straßenverkehr zu sein. Wichtig ist ein direkter, aktiver Dialog zwischen den Beteiligten (Kind, Eltern, Schule, Polizei). Auch wenn die Verantwortung für die Sicherheit auf dem Schulweg in erster Linie bei den Erziehungsberechtigten liegt, sollte bei der Entscheidung von Erziehungsberechtigten für oder gegen eine Nutzung der Schutzranzen-App berücksichtigt werden, dass sich die Beteiligten auf ein technisches Gerät verlassen, statt auf ihre Sinne. Das kann unter Umständen zu einem unvorsichtigeren Verhalten im Straßenverkehr als ohne die App führen. Das Kultusministerium sieht keine Notwendigkeit, derartige Apps zu bewerben oder zu unterstützen.

8. Sollten ihrer Auffassung nach auf satellitengestützten Standortdaten basierende Programme und Apps, welche dazu dienen, autonom fahrende Autos weiterzuentwickeln, zugelassen werden, auch wenn diese Technologien durch datensparsamere Sensorik ersetzt werden können?

Das Kultusministerium empfiehlt derartige Apps aus den bereits erwähnten Gründen nicht. Zur Bewertung dieses Sachverhaltes liegen dem Verkehrsministerium keine Erkenntnisse vor.

9. Wie bewertet sie die Aussage des App-Anbieters, die betroffenen Schulkinder könnten in den Einstellungen der App selbst darüber entscheiden, wann sie der Überwachung unterliegen bzw. wann nicht, mit Blick auf die Mündigkeit und das Problembewusstsein insbesondere jüngerer Schulkinder?

Minderjährige Schülerinnen und Schüler üben alle Rechte des Datenschutzes selbst aus, sofern sie die nötige Einsichtsfähigkeit hierfür besitzen. Ansonsten werden diese Rechte durch deren Erziehungsberechtigte ausgeübt. Die Einsichtsfähigkeit ist nach dem jeweiligen Reifezustand der Schülerin bzw. des Schülers und dem Verwendungszusammenhang der Daten zu beurteilen. Sie liegt nicht vor, wenn diese die Folgen einer Verarbeitung personenbezogener Daten nicht erkennen und nicht sachgerecht einschätzen können. Mit Vollendung des 16. Lebensjahres ist in der Regel vom Vorliegen der nötigen Einsichtsfähigkeit auszugehen. In Zweifelsfällen hat der Empfänger der Einwilligungserklärung zu prüfen, ob die Einsichtsfähigkeit tatsächlich vorliegt (vgl. unter II., 1.1 bis 1.3 der Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ vom 5. Dezember 2014; s. nunmehr auch Art. 8 Abs. 1 DSGVO).

Die hinter dieser für die Verarbeitung personenbezogener Daten durch öffentliche Schulen geltenden Bestimmung stehenden allgemeinen Rechtsgedanken können auf den vorliegenden Zusammenhang übertragen werden. Mangels datenschutzrechtlicher Verantwortlichkeit des Kultusministeriums und der nachgeordneten Schulaufsichtsbehörden sowie der Schulen enthält sich das Kultusministerium einer Bewertung der Aussage des App-Anbieters.

Dr. Eisenmann

Ministerin für Kultus,
Jugend und Sport

Anlage

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT
03/2018

Leitfaden für die datenschutzkonforme Auswahl und Nutzung von Apps

Die Auswahl und Nutzung von Apps gehen mit der Beurteilung komplexer datenschutzrechtlicher Fragestellungen einher. Die vorliegende Handreichung soll Schulen und andere Stellen dabei unterstützen, datenschutzkonforme Apps zu *identifizieren* bzw. auszuwählen und eine Nutzung entsprechend den gesetzlichen Vorgaben zu gewährleisten.

Allerdings wird an dieser Stelle darauf hingewiesen, dass datenschutzrechtliches und informationstechnisches Grundwissen vorhanden sein muss, um diese Auswahl sachgerecht treffen zu können. Das vorliegende Dokument kann hierfür als Hilfestellung dienen.

Apps können von Schulen aus didaktisch-pädagogischen Gründen, aber auch zu Verwaltungszwecken (z.B. mobiler Lehrerkalender) genutzt werden. Der Einsatz wird u. a. durch § 1 SchG (Erziehungs- und Bildungsauftrag) abgedeckt. Die durch die App verarbeiteten personenbezogenen Daten müssen zur Aufgabenerfüllung tatsächlich auch erforderlich sein, d.h. die Aufgabe kann ohne diese Daten nicht oder nicht sachgerecht erfüllt werden. Eine bloße Nützlichkeit würde nicht ausreichen, die personenbezogenen Daten zu verarbeiten. Die verarbeiteten Daten dürfen nur für diese Zwecke genutzt werden, eine darüber hinausgehende Verarbeitung ist unzulässig.

Für eine datenschutzrechtliche Bewertung von Apps ist es zunächst wichtig, zu wissen, ob personenbezogene Daten ausschließlich lokal auf dem Gerät, auf welchem die App installiert ist, verarbeitet werden (darunter fällt auch eine Speicherung), oder (auch) bei einem Dienstleister, z. B. auf dessen zentralem Server. Dann liegt eine Auftragsverarbeitung von personenbezogenen Daten vor, für die eine spezielle datenschutzrechtliche schriftliche Beauftragung erfolgen muss (Vorlagen hierfür finden Sie auf it.kultus-bw.de oder dem Lehrerfortbildungsserver). Eine bloße Einwilligung in AGB genügt in der Regel nicht.

Generell gilt, dass die jeweilige Schule immer die datenschutzrechtlich verantwortliche Stelle bei der Nutzung der App bleibt - auch dann, wenn bei der Verwendung der App ein Dienstleister die Datenverarbeitung durchführt. Das bedeutet, dass die Schule die Rechtmäßigkeit der Datenverarbeitung sicherstellen muss. Die Rechtmäßigkeit bezieht sich insbesondere auf Art und Umfang der Datenverarbeitung, also darauf, welche personenbezogenen Datenarten auf welche Weise verarbeitet werden. Darüber hinaus ist auch auf die Art und Weise und den Zweck eventueller Übermittlungen zu achten. Zu prüfen ist z. B., ob eine Datenübermittlung zu Werbezwecken erfolgt, wie es bei vielen Apps der Fall ist. Dies wäre beim Einsatz an Schulen unzulässig. Die Schule muss auch sicherstellen, dass technische und organisatorische Datenschutzmaßnahmen nach Art. 32 Abs. 1 EU-DSGVO getroffen werden, z. B. die

Verhinderung unbefugten Zugriffs. An erster Stelle sei hier genannt, dass die Daten zwingend verschlüsselt sein müssen, wenn diese auf einem mobilen EDV-Gerät gespeichert werden.

Ferner ist die Schule dafür verantwortlich, folgende Rechte der Betroffenen zu wahren

- Auskunftsrecht (Art. 15 EU-DSGVO)
- Recht auf Berichtigung (Art. 16 EU-DSGVO)
- Recht auf Löschung (Art. 17 EU-DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 EU-DSGVO)
- Datenübertragbarkeit (Art. 20 EU-DSGVO)
- Widerspruchsrecht (Art. 21 EU-DSGVO)

Das bedeutet, dass die Schule in all diesen Fällen die Betroffenen bzw. auskunftsberechtigten Personen nicht an den Dienstleister oder gar den Programmierer der App verweisen darf, sondern selbst handeln muss.

Die folgenden Kriterien und Hinweise helfen bei der Auswahl einer geeigneten und vor allem datenschutzrechtlich zulässigen App:

	Muss	**Soll**
1. Techn. Eigenschaft der App		
Für welche Betriebssysteme steht ggf. die App zur Verfügung? ○ iOS ○ Android ○ Windows Phone ○ sonstige		 O O O O
Ist es möglich, die App pseudonymisiert oder anonymisiert zu nutzen? *Dies ist dann notwendig, wenn für die Nutzung der von der App vorgesehenen Funktion keine personenbezogenen Daten erforderlich sind, beispielsweise bei einer App zur Simulation physikalischer Experimente.*		O
Ist das Passwort ausreichend komplex? (mind. 6 Stellen, Ziffer, Kombination aus Groß- und Kleinbuchstaben) Kann das Passwort bei der Eingabe maskiert werden? Erfolgt keine Speicherung des Passworts im Klartext auf dem Gerät?	O O O	
Wird klar (z.B. aus einer technischen Beschreibung) welche personenbezogenen Daten verarbeitet werden? • *Techn. Daten wie IP, IMEI, UDID, IMSI, MAC-Adresse,*	O	

MSISDN, Name des Telefons, Standortdaten, biometrische Daten (Fingerabdruck), Daten zur Nutzung der App (wer hat sie wann genutzt?) • *Aber auch die Daten, die die App für den Anwender verarbeitet im Sinne der funktionalen Sicht auf die App, sog. Inhaltsdaten.*		
Kann bei der Nutzung der App, z.B. durch Deaktivieren / Abschalten, ein unzulässiger Zugriff auf weitere auf dem Gerät gespeicherte personenbezogene Daten ausgeschlossen werden? Z. B. Daten von auf dem Gerät gespeicherten Kontakten, Bildern oder anderen Dateien. *Ein solcher Zugriff ist grundsätzlich nur dann zulässig, wenn dies erforderlich ist, um den Zweck (schulischer Erziehungs- und Bildungsauftrag) zu erfüllen.* *Dabei ist auch der nächste Punkt zu berücksichtigen.*	O	
Ist gewährleistet, dass keine personenbezogenen Daten von unbeteiligten dritten Personen verarbeitet werden, z.B. Daten einiger Betroffener aus den lokal auf dem Gerät gespeicherten Kontakten oder Anruflisten?	O	
Ist es möglich, den Zugriff auf zur Nutzung nicht unbedingt erforderliche Gerätefunktionen zu verhindern? *Für die bloße Nutzung eines Messengers ist beispielsweise kein Zugriff auf die Ortungsfunktion und damit die Standort-Daten erforderlich*	O	
Sofern personenbezogene Daten lokal auf dem Gerät gespeichert werden: Ist eine verschlüsselte Speicherung sichergestellt?	O	
Erfolgt die Kommunikation, bei der personenbezogene Daten ausgetauscht werden, über verschlüsselte Verbindungen (SSL-Zugang, IPSec-VPN)?	O	
Kann der Zugang / die Anmeldung an der App durch ein zusätzliches Authentifizierungsmerkmal (z.B. Hardware/Software-Token) abgesichert werden?		O
Bietet die App die Funktion, Daten sicher und endgültig zu löschen?	O	
Gibt es eine Möglichkeit, die lokal gespeicherten Daten zu sichern (Backup-Funktionalität)? *Auch dabei sind datenschutzrechtliche Aspekte zu beachten: Erfolgt die Datensicherung in einer Cloud oder bei einem Dienstleister, liegt eine Auftragsdatenverarbeitung vor, ein entsprechender Vertrag ist abzuschließen. Ggf. kann die Datensicherung auch auf dem eigenen PC erfolgen.*		O

	Muss	Soll
2. AGB / Nutzungsbedingungen		
Ist ausgeschlossen, dass sich der Entwickler der App vorbehält, den Umfang der verarbeiteten Datenarten zu ändern, ohne die Anwender hierüber zu informieren?	O	
Ist ausgeschlossen, dass personenbezogene Daten an Dritte zu weiteren Zwecken (z.B. Werbung) übermittelt werden? *Eine Weitergabe von personenbezogenen Daten an Dritte ist unzulässig!* *Hinweise hierauf können sich aus den AGBs oder Systembeschreibungen ergeben.*	O	

Die folgenden Kriterien sind zu berücksichtigen, wenn die App auch personenbezogene Daten auf einem Server bei einem Dienstleister verarbeitet (auch gespeichert), z.B. bei der Verwendung sog. Clouds.		
	Muss	**Soll**
Besteht für die Datenübertragung zwischen mobilem Endgerät und zentralem Server eine Ende-zu-Ende Verschlüsselung?	O	
Bietet der Dienstleister ausreichend Gewähr für eine datenschutzgerechte Datenverarbeitung? Hierbei helfen folgende Leitfragen: • Verfügt er über Datenschutz Know-How? • Gab es in der Vergangenheit keine bei dem Dienstleister bekannt gewordenen Datenschutzpannen oder technische Missstände?	O	
Liegt eine Zertifizierung (z.B. nach BSI Grundschutz oder ISO 27001, bzw. ISO 27018) vor für das Rechenzentrum, in welchem eine Datenverarbeitung bei der Nutzung der App erfolgt? *Die Schule muss sich von den vom Dienstleister getroffenen technischen und organisatorischen Maßnahmen überzeugen. Wenn die Schule nicht die Mittel und Möglichkeiten hat, die ordnungsgemäße Verarbeitung ihrer Daten beim Dienstleister zu überprüfen, könnten aktuelle und aussagekräftige Nachweise von anerkannten und unabhängigen Prüfungsorganisationen herangezogen werden.* *Hierzu gehört insbesondere eine Zertifizierung nach BSI-Grundschutz + Baustein Datenschutz oder ISO 27001 (dann muss der Baustein Datenschutz durch die Schule geprüft werden, siehe Hinweis des KM zur Zertifizierung bei einer ADV).*		O
Befinden sich der Sitz des Dienstleisters und der Standort der Server innerhalb des Geltungsbereichs der EU-DSGVO oder in einem Land mit einem damit vergleichbaren Datenschutzniveau?	O	

Eine Verarbeitung personenbezogener Daten von Schulen außerhalb dieser Länder muss grundsätzlich unterbleiben und ist nur im Ausnahmefall (z.B. Auslandsschule) mit Zustimmung des KM zulässig.		
Lässt es der Dienstleister zu, dass sich die Schule von der Einhaltung der Datenschutzmaßnahmen selbst überzeugen kann? *Dies kann z.B. durch eine Begehung und Prüfung des Rechenzentrums vor Ort erfolgen. Der Dienstleister darf eine solche Kontrollmöglichkeit nicht untersagen.*	O	
Es gibt keine Anzeichen, dass der Dienstleister personenbezogene Daten an Dritte z. B. zu Werbezwecken übermittelt. *Informationen über solche Übermittlungen sind meist in den Nutzungsbedingungen aufgeführt.*	O	
Ist eine schriftliche, datenschutzkonforme Erteilung des Auftrags für die Auftragsdatenverarbeitung möglich? *Es handelt sich aus datenschutzrechtlicher Sicht um eine sog. Auftragsdatenverarbeitung (Art. 28 EU-DSGVO).* *Viele Dienstleister ermöglichen lediglich die Einwilligung in bzw. das Akzeptieren von vorgefertigten AGBs bzw. Nutzungsbedingungen. In der Regel genügen solche AGBs bzw. Nutzungsrichtlinien nicht den datenschutzrechtlichen Vorgaben des Art. 28 EU-DSGVO.* *Das KM empfiehlt, einen Vertrag entsprechend der unter www.it.kultus.bw.de oder auf dem Lehrerfortbildungsserver bereit gestellten Vorlagen abzuschließen.*		
Teilt der Dienstleister konkret die eingesetzte Hardware, Software und die Art der Vernetzung mit?	O	
Benennt er, wo sich das Rechenzentrum befindet?	O	
Werden die vom Dienstleister getroffenen technischen und organisatorischen Datenschutzmaßnahmen konkret und nachvollziehbar dargestellt?	O	
Existiert eine schriftliche oder elektronische Dokumentation bezüglich der beim Dienstleister vorhandenen Technik und Funktionalität?	O	
Macht der Dienstleister **konkrete** Angaben über ggf. vorhandene Unterauftragsverhältnisse und werden die Unternehmen benannt? *Die Schule muss über alle Unterauftragsverhältnisse, sofern diese vorgesehen sind, informiert sein.*	O	
Lässt er zu, dass ggf. weitere Unterauftragnehmer nur nach Zustimmung der Schule beteiligt werden dürfen?	O	
Besitzt die Schule die vertraglich gesicherte Befugnis, dem Dienstleister hinsichtlich der Verarbeitung personenbezogener Daten Weisungen zu erteilen?	O	
Stellt der Dienstleister dar, nach welchem Datensicherungskonzept die in der Plattform liegenden Nutzerdaten gesichert werden? *Hierzu sollte der Dienstleister das eingestellte Sicherungsverfahren darstellen.*	O	

Sollten Antworten zu den oben genannten Aspekten nicht vorliegen oder sollte sich die Schule nicht in der Lage sehen, diese Punkte zu beurteilen, so sollte von einer Nutzung bzw. Beauftragung abgesehen werden.
Fehlt eines der obigen Muss-Kriterien, ist ebenso von einer Beauftragung abzusehen.

Tipps für den Betrieb:

- Das jeweilige Gerät / System sollte so konfiguriert sein, dass das **Installieren von Updates von Apps** erst nach Freigabe durch den Anwender erfolgt. Dabei ist zu prüfen, ob und was sich am (funktionalen) Umfang der App geändert hat. So könnten beispielsweise weitere Datenarten verarbeitet werden oder die App wünscht Zugriff auf weitere Systemressourcen wie Kalender oder Kontakte.
- **Logs** sollten regelmäßig gelöscht werden, sofern personenbezogene Daten verarbeitet werden. Es wird eine Löschfrist von 7 bis 14 Tagen empfohlen.
- Sofern die App über eine Möglichkeit zur **Speicherung des Passworts** verfügt, darf dies nicht genutzt werden.
- Wird an der Schule eine App eingeführt, so ist ggf. der örtliche Personalrat zu beteiligen. Über den Einsatz der App sollten Schülerinnen und Schüler, sowie die Eltern informiert werden. Hierfür bietet sich der Elternabend an.

Begriffs- und Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BSI	Bundesamt für die Sicherheit in der Informationstechnik
IMEI	Gerätenummer, International Mobile Equipment Identity
IMSI	Kartennummer, International Mobile Subscriber Identity
IP	Netzwerkadresse Internet Protocol
IPSec	(Internet Protocol Security) Protokoll, welches eine gesicherte Kommunikation über potentiell unsichere Netze wie das Internet ermöglicht
ISO	Internationale Organisation für Normung
LDAP	(Lightweight Directory Access Protocol) Anwendungsprotokoll aus der Netzwerktechnik zur Abfrage und Modifikation von Informationen eines Verzeichnisdienstes (eine im Netzwerk verteilte hierarchische Datenbank) über ein IP-Netzwerk.
LDSG	Landesdatenschutzgesetz Baden-Württemberg
MAC	Hardware-Adresse eines Netzadapters, Media Access Control Adress
MSISDN	Mobilfunknummer, Mobile Subscriber IDSN Number
SSL	(Secure Sockets Layer) hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS (Transport Layer Security) weiterentwickelt und standardisiert
UDID	Gerätenummer eines iOS Geräts, Unique Device ID
VPN	(Virtual Private Network) privates (in sich geschlossenes) Rechnernetz, das auf einer öffentlichen Netzwerk-Infrastruktur (z.B. Internet) aufgebaut ist