Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Postsendungen bitte an die Postanschrift des TLfDI, Postfach 900455, 99107 Erfurt!

Thüringer Landesbeauftragter für den Datenschutz und
die Informationsfreiheit (TLfDI), PF 900455, 99107 Erfurt

AZ: 438-17/2021-4.1

(Aktenzeichen bei Antwort angeben)

An die Schulleitungen der Thüringer Schulen

Per E-Mail lt. Verteiler

Ihre Nachricht vom :
Ihr Zeichen :
Bearbeiter/in :
Telefon :
Erfurt, den : 17. März 2021

Weitere Informationen und Hinweise zu schulischen Softwareprodukten

Sehr geehrte Schulleiterinnen,
sehr geehrte Schulleiter,

seit dem letzten Schreiben des TLfDI vom 29.01.2021, Az.: 438-17/2021-3.1 zu verschiedenen Softwareprodukten für schulische Zwecke hat den TLfDI wieder eine überwältigende Menge an Fragen zur Zulässigkeit der Nutzung von weiteren Schulsoftwareprodukten erreicht. Die vorliegende Information soll als Multiplikatoreffekt dienen, damit der TLfDI nicht die Fragen nach gleichen Produkten mehrfach beantworten muss. Wie in den letzten Schreiben bitte ich Sie auch diesmal wieder, den Lehrkräften an Ihrer Schule die Informationen ebenfalls zugänglich zu machen.

Zunächst möchte ich auf einen Fehler aufmerksam machen, der uns bei der Aufzählung von Messenger-Diensten im Schreiben vom 15.01.2021, Az.: 438-121/2020.6 unterlaufen ist. Dort wurde versehentlich der Messenger-Dienst „**Textsecure**“ genannt. Gemeint war aber der Dienst „**Chatsecure**“. **„Chatsecure“** ist ein anderer Messenger-Dienst, der unter iOS läuft und aus datenschutzrechtlicher Sicht **Verwendung finden kann**. Das Gegenstück für Android nennt sich **Conversations**. Beide Apps können auch untereinander Nachrichten austauschen und sind interoperabel.

Postanschrift: Postfach 900455, 99107 Erfurt
Dienstgebäude: Häßlerstraße 8, 99096 Erfurt
Telefon: 0361 57-3112900
Telefax: 0361 57-3112904
E-Mail*: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

*Die genannte E-Mail-Adresse dient nur für den Empfang einfacher Mitteilungen ohne Signatur/ Verschlüsselung und für mit PGP verschlüsselte Mitteilungen.

Weiterhin war vor kurzem der Presse zu entnehmen, dass in der Lernapp **„Anton“** eine Sicherheitslücke entdeckt wurde, die aber inzwischen bereits von der Entwicklungsfirma wieder geschlossen worden sein soll. Es sollen auch keine Hinweise auf Datenabflüsse festgestellt worden sein. Vor Sicherheitslücken und Hackerangriffen auf Lernapps und Lernplattformen ist man leider nie 100%ig geschützt. Wichtig aus Sicht des Datenschutzes ist, dass auf die bekannt gewordenen Lücken kurzfristig, transparent und hinreichend reagiert wird. Dies ist bei Anton der Fall. Der TLfDI macht zum Maßstab seiner kursorischen Prüfungen von Schulsoftware immer die Einhaltung von datenschutzrechtliche Regelungen durch die App und den Umgang der App mit personenbezogenen Daten der Nutzer. Wenn bereits nach der „Papierform“ Verstöße erkennbar werden, kann ein solches Produkt nicht empfohlen werden.

1. Gegen die Nutzung der nachfolgenden Apps zu schulischen Zwecken, allerdings unter Berücksichtigung unter den jeweils genannten Voraussetzungen bestehen **derzeit keine durchgreifenden Bedenken**:

Sdui: Hier ist eine datenschutzkonforme Nutzung derzeit grundsätzlich möglich. Es besteht aber das Problem, dass das US-amerikanische Cloudprodukt „Cloudflare“ genutzt wird. Der TLfDI hat den Anbieter angeschrieben und Vorschläge unterbreitet, welche anderen Lösungen in Frage kämen. Sollte der Anbieter hierauf eingehen, kann das Produkt für Thüringer Schulen empfohlen werden.

Terminplanungsmodul „**dudle**“ der Technischen Universität Dresden. Eine datenschutzkonforme Nutzung ist grundsätzlich möglich, etwa zur Terminabstimmung zwischen Schule und Eltern. Leider bietet die TU Dresden keinen Auftragsverarbeitungsvertrag (AVV) an, noch kann ein AVV mit der TU Dresden abgeschlossen werden. Ein Betrieb auf dem schul- bzw. schulträgereigenen Server wäre aber möglich und würde auch hinsichtlich der Installation und Einrichtung von der TU Dresden unterstützt werden.

Bei **oncoo.de** wurde derzeit kein Tracking, keine Datenübermittlung an Dritte und keine unsicheren Drittanfragen gefunden. Es wird ein in Deutschland betriebener Server genutzt. Nach kursorischer Prüfung bestehen gegen die Nutzung derzeit keine datenschutzrechtlichen Bedenken.

Bei **LearningApps.org** ließen sich derzeit ebenfalls kein Tracking und keine Werkzeuge von Drittanbietern feststellen. **Google Analytics** kann **deaktiviert** werden. Es wurden derzeit keine Punkte gefunden, die eine Nutzung zu schulischen Zwecken unzulässig erscheinen.

LearningView.org hat derzeit keine Cookies zu Tracking- oder Werbezwecken, sondern nur technisch notwendige Cookies. Zum Prüfzeitpunkt war der Standort des genutzten Servers in Deutschland. Bis auf weiteres kann die Apps für den Unterricht eingesetzt werden.

EduPage (https://www.asc-raabe.de/edupage) war bereits im Schreiben vom 15.01.2021 angesprochen worden. Hierzu ist zu ergänzen, dass **Google Analytics** Anwendung findet und von der Schule **im Auftragsverarbeitungsvertrag ausgeschlossen werden muss**.

Das Videokonferenzsystem „**TeamViewe**r“ ist technisch derzeit sicher, der von der Firma zur Verfügung gestellte **Muster-Auftragsverarbeitungsvertrag sollte aber nicht verwendet werden** und stattdessen ein eigener Auftragsverarbeitungsvertrag mit „Teamviewer“ abgeschlossen werden.

Ausdrücklich verweise ich darauf, dass für jedes Schultool, welches eine Schule nutzt, ein Auftragsverarbeitungsvertrag erstellt werden muss. Falls erforderlich, sollte die Schule juristische Unterstützung im zuständigen Staatlichen Schulamt angefordert werden. Das Muster eines Auftragsverarbeitungsvertrags ist auf der Internetseite des TLfDI unter:
https://www.tlfdi.de/mam/tlfdi/themen/tlfdi_formulierungshilfe_fur_auftragsverarbeitungsvertraege.pdf abzurufen.

2. Bedenken bestehen indes bei folgenden Produkten:

Bei der Nutzung von **Microsoft 365** bzw. des Videokonferenztools **Microsoft Teams** wäre in jedem Fall ein Auftragsverarbeitungsverhältnis gemäß Art. 28 DS-GVO zwischen der Schule (Verantwortlicher im Sinne von Art. 4 Ziffer 7 DS-GVO) und dem Auftragsverarbeiter (hier Microsoft Deutschland GmbH) zu begründen. Gegenwärtig spricht indes vieles dafür, dass der (Muster-)Auftrags-verarbeitungsvertrag zwischen „dem Kunden" als Verantwortlichem und MS als Auftragsverarbeiter **verschiedene Unklarheiten** enthält. Die Problematik wurde bereits unter den Datenschutzbeauftragten des Landes und des Bundes diskutiert, eine abschließende Entscheidung ist hierzu aber noch nicht erfolgt. Ob die von der Berliner Beauftragten für Datenschutz und Informationsfreiheit geäußerte Kritik (siehe Link unten) zu einer Unzulässigkeit von MS Teams und im Weiteren auch zur Unzulässigkeit von MS 365 führen wird und daher auch die Nutzung dieses Verfahrens den Schulen untersagt werden muss, ist daher derzeit noch unklar. Die aktuellen Positionen und Materialien zu Videokonferenzsystemen von der Berliner Landesbeauftragten sind auf der Seite https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf ausführlich dargelegt.

Darüber hinaus hat sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) zu diesem Thema bereits geäußert: https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf, dort Anlage 1. Dieser rechtlichen Auffassung schließt sich der TLfDI an, insbesondere auch für den Bereich Schule. Möglicherweise wird sich die DSK in absehbarer Zeit abschließend äußern.

Bis dahin verweisen wir auf die Position Ihres Dienstherrn in den FAQ des TMBJS „Datenschutz in Schulen". Dort wird, unter Punkt 7.5 unter anderem die **Verwendbarkeit von Office 365 (damit auch MS Teams) derzeit verneint**.

Da den TLfDI häufig Anfragen nach dem Videokonferenzsystem **Zoom Meeting** (https://zoom.us) erreichen, soll darauf hingewiesen werden, dass trotz positiver Bemühungen **keine datenschutzkonforme Nutzung in der EU möglich** ist. Beispielsweise liegen Mängel im vorgegebenen Auftragsverarbeitungsvertrag, unzulässige Einschränkungen der Weisungsbindung, der Löschpflicht und der Kontrollrechte vor. Insbesondere ist auf die unzulässigen Datenexporte von Zoom Meeting hinzuweisen. Es wird hier auf das o. g. Papier der Berliner Beauftragten für Datenschutz und Informationsfreiheit in der Version 2.0 vom 18.02.2021 auf den Seiten 6 und 33-35 verwiesen.

"**sofatutor**" (Lernprogramm für verschiedene Fächer und Klassenstufen) ist ein deutscher Anbieter aus Berlin, der mögliche Übertragungen zu Dritten auf das sog. „Privacy Shield" stützt, welches vom Europäischen Gerichtshof für ungültig erklärt wurde. Zudem nutzt sofatutor Google Analytics, Convert Insights, Scout (alle USA). Dies wird als derzeit nicht datenschutzkonform bewertet.

YouTube Videos im Unterricht: Dies ist immer mit einer Datenübertragung in USA verbunden, für die keine Rechtsgrundlage existiert. **Zusätzlich schließen die Nutzungsbedingungen von Youtube jegliche NICHT private Nutzung aus**.

Auf **kialo-edu.com**, kann man Diskussionsbeiträge zu z. B. von Lehrern vorgegebenen Themen einstellen, etwa zum Üben des Diskutierens. Leider muss aus der Sicht des TLfDI derzeit von der Nutzung abgeraten werden, da der Server in den USA steht und das Verfahren nach eigenen Angaben des Anbieters nicht DS-GVO-konform ist.

Bei **duolingo.com** erfolgt eine Übertragung von Daten in die USA zu einem bei Amazon gehosteten Server. Es wird Google Analytics eingesetzt sowie 17 weitere Analyse und Werbeanbieter. Daher ist derzeit eine datenschutzkonforme Nutzung in Schulen nicht möglich.

Auf **quizlet.com** werden 120(!) Cookies beim Besuch der Website gesetzt. Diese ist mit zahlreichen Tracking, Analyse und Werbediensten bestückt. Daher wird ebenfalls die Nutzung derzeit als nicht zulässig angesehen.

Auf **schooltogo.de** wird Google-Analytics eingesetzt. Die Analyse wird auch in der Datenschutzerklärung angegeben, siehe https://schooltogo.de/datenschutz/. Das Tracking kann nicht deaktiviert werden. Daher kann derzeit keine datenschutzrechtliche Empfehlung erteilt werden.

Bei **schlaukopf.de** wird Google Analytics, DoubleClick.net (Werbung) und Amazon Ads genutzt. Auch ohne Einwilligung (und aktiver Abschaltung) sind diese Dienste aktiv. Technisch ist damit die Einwilligung fehlerhaft umgesetzt. Daher kann die Nutzung derzeit nicht empfohlen werden.

frustfrei-lernen.de lässt 100 Partner für Analytics und Werbung zu. Diese sind auch nicht vollständig unterdrückbar. Daher wird von der Nutzung derzeit abgeraten.

Bei **quizacademy.de/www.quizacademy.org** gibt es 14 externe Empfänger von Daten (u.a. Google Analytics und DoubleClick.net). Dem Tracking kann nicht widersprochen werden. Daher wird von der Nutzung derzeit ebenfalls abgeraten.

wooclap.com: Es lässt sich der Einsatz von Google-Analytics und DoubleClick.net feststellen. Der Serverstandort ist in den USA. Im Ergebnis wird von der Nutzung derzeit abgeraten.

TeacherMade.com stammt von einem US-amerikanischen Hersteller, ist nicht datenschutzkonform und kann aus der Sicht des TLfDI derzeit nicht empfohlen werden.

In **G-Suite for Education** ist **Google Drive** unter andere Standarddienste von Google enthalten. Es wird zwar ein separater Auftragsverarbeitungsvertrag ange-

boten, welcher in Teilen aber wieder auf die Standardverarbeitungszwecke von Google verweist. Es sind Verarbeitungszwecke vorgesehen, die keine schulischen Zwecke sind. Es gibt eine Stellungnahme des TLfDI ggü. Google, die aber noch nicht beantwortet wurde.

Edhu.school (https://edhu.school/) bietet eine "All-In-One-Lösung für Schulen", d. h. für pädagogische- und Verwaltungsaufgaben in einer Anwendung. Hier besteht, wie bei anderen Anbieten auch, immer die Gefahr der Vermischung beider Aufgabenbereiche. Der Anbieter verweist auf seine DS-GVO-Konformität, aber die Datenschutzerklärung ist unvollständig. Es ist unklar, ob ein Auftragsverarbeitungsvertrag geschlossen werden kann. Es kann derzeit keine datenschutzrechtliche Unbedenklichkeit zur Nutzung der App ausgesprochen werden.

onilo.de/ (Storydocks GmbH Hamburg - digitale Geschichten zur Sprach- und Leseförderung, Unterrichtsideen): Nach der Datenschutzerklärung findet eine Verarbeitung personenbezogener Daten derzeit nur im EU-Gebiet statt. Leider gibt es eine Facebook-Anbindung und in Webinaren werden Verbindungen zu Facebook, Google, Twitter u.a. aufgebaut. Daher kann die App derzeit nicht empfohlen werden

Bei **serlo.org** lässt sich kein Tracking feststellen. Es wird allerdings Cloudflare als Content-Delivery-Network eingesetzt. Der Serverstandort ist damit die USA. Daher kann in dieser Form leider derzeit ebenfalls keine Empfehlung abgegeben werden.

Adobe.scan übermittelt die Daten zur Analyse in die USA. Da „Adobe Scan" Texterkennung und Bildverbesserung unterstützt, muss davon ausgegangen werden, dass dies auch auf Servern in den USA geschehen kann. Daher wird die Nutzung dieser App derzeit nicht empfohlen.

Instagram ist ein Online-Dienst von Facebook Inc., Menlo Park, Kalifornien. Bei der Nutzung von Instagram werden mit jedem Hochladen von Inhalten aber auch beim Nur-Lesen-Zugriff Daten aus dem Endgerät des Nutzers an Server in den

USA übertragen. Nach Untersuchungen beim TLfDI wird bei Instagram jede Aktion des Nutzers (und auch Inaktivität) an graph.instagram.com gesendet. Diese Aktionen sind mit Geräte- und Nutzer-IDs versehen und damit personenbezogen. In den sogenannten Facebook-Services werden dienst-übergreifend mehrere Analysedienste, etwa Facebook Analytics (https://analytics. facebook.com/) und Facebook Insights (https://de-de.facebook.com/business/ insights/tools/audience-insights) betrieben, die unter „Facebook-IQ" vermarktet werden. Davon ist auch Instagram betroffen. Hier werden auf Einwilligungsbasis der Nutzer aus den Nutzerdaten (d. h. eingestellte Nutzerinhalte, aber auch die Nutzeraktionen auf dem Service) Eigenschaften über diese Nutzer gesammelt. Zusätzlich räumt sich Instagram das Recht ein, eingestellte Fotos nach eigenem Belieben nutzen zu dürfen. Fakt ist, dass damit praktisch keinerlei Steuerungsmöglichkeiten für eingestellte Inhalte bestehen. Man lasse sich nicht dadurch täuschen, dass man ja selbst Inhalte „löschen" kann. Niemand kann von außen auf einem US-Server prüfen, ob und was tatsächlich gelöscht wurde. Von der schulischen Nutzung von Instagram wird datenschutzrechtlich abgeraten.

Facebook ist ebenfalls ein US-amerikanisches Produkt, das die Daten in den USA verarbeitet und Nutzerdaten verwertet. Die Nutzung von Facebook für schulische Zwecke ist nicht zulässig, was sich bereits herumgesprochen haben müsste.

WhatsApp ist ein verbreiteter Messenger-Dienst, der zwar eine Ende-zu-Ende Verschlüsselung anbietet, aber Metadaten verarbeitet und die Kontakte auf dem Smartphone ausliest. Es werden die Daten mit Facebook geteilt. Das TMBJS hat den Dienst in seinen FAQ unter 14.1 **untersagt**.

Selbstverständlich können Sie weitere Fragen zu Schulapps an den TLfDI richten. Es wird aber gebeten, zunächst abzuklären, ob in den bereits herausgegebenen Schreiben an die Schulleitungen datenschutzrechtliche Einschätzungen zu einem bestimmten Verfahren gegeben wurden.

Sie können auch selbständig ein Screening der App durchführen, indem Sie auf die Seite https://webbkoll.dataskydd.net/de/ gehen und die Internetadresse des entsprechenden Tools eingeben. Es werden dann die Datenschutzfunktionen der Website geprüft. Interessant ist dann insbesondere, wo der Server steht und welche Dritten die Daten ebenfalls erhalten. Wie mehrfach dargelegt, ist bei Servern mit Standort in den USA oder bei Zugriffen auf Servern durch US-amerikanische Firmen in der Regel nach der derzeitigen Rechtslage von der Nutzung der App zu dienstlichen/schulischen Zwecken abzuraten.

Weitere Erkenntnisse des TLfDI werden Ihnen in neuen Rundschreiben mitgeteilt.

Mit freundlichen Grüßen
im Auftrag