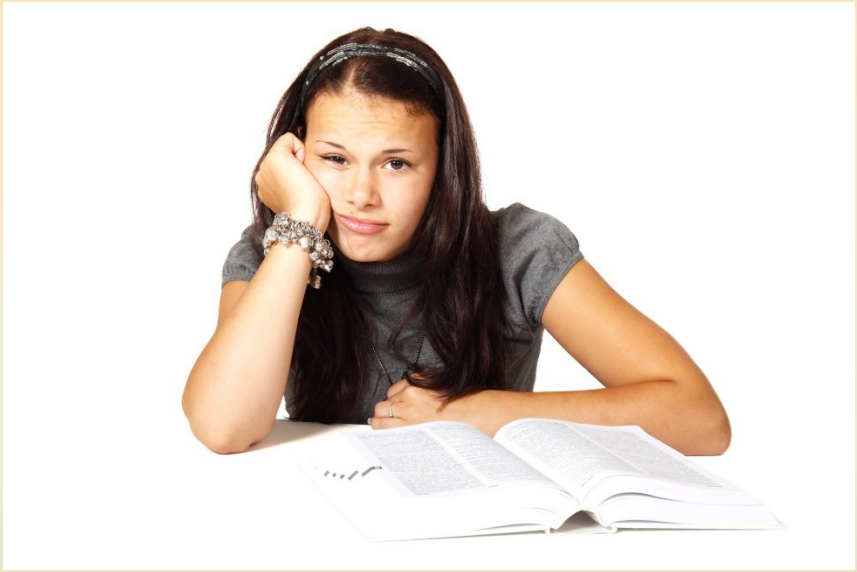
Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Datenschutz und Schule



Dr. Lutz Hasse – TLfDI

Gliederungspunkte

- Recht
- Probleme
- Wie geht es weiter?

- Kosinski-Clip

(Prof. Michal Kosinski „Die Digitalisierung und ihre Auswirkung auf Mensch und Gesellschaft“)

BVerfGE 65, 1 – Volkszählungsurteil (15. Dezember 1983) = wichtigstes Urteil für den Datenschutz in Deutschland

- BVerfG hat eine Ausprägung des Persönlichkeitsrechts neu definiert: Aus dem Grundrecht der Menschenwürde (Art. 1 Abs. 1 GG) und dem Grundrecht auf allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) hat BVerfG ein Recht auf informationelle Selbstbestimmung herausgebildet.

Auszug aus dem Urteil:

„Mit dem Recht auf informationelle Selbstbestimmung wäre […] eine Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst.“ (…)

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

„…, insoweit gibt es unter den Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr.“

Verfassung des Freistaats Thüringen

Artikel 6

(2) Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Er ist berechtigt, über die Preisgabe und Verwendung solcher Daten selbst zu bestimmen.

(3) Diese Rechte dürfen nur auf Grund eines Gesetzes eingeschränkt werden. Den Belangen historischer Forschung und geschichtlicher Aufarbeitung ist angemessen Rechnung zu tragen.

Personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Die Schulen verarbeiten zur Aufgabenerfüllung in diesem Sinn Schüler-, Lehrer- und Elterndaten.

Verarbeitung gemäß Art. 4 Nr. 2 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Schule als „Verantwortlicher“ gemäß Art. 4 Nr. 7 DS-GVO

„Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

In diesem Sinn ist die Schule „Verantwortlicher“ für die Verarbeitung von Schüler-, Lehrer- und Elterndaten.

Nach § 33 ThürSchulG vertritt die Schulleitung die Schule nach außen und ist u. a. gegenüber dem Lehrpersonal weisungsberechtigt.

Auch gemäß Art. 29 DS-GVO darf jede dem Verantwortlichen unterstellte Person diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten.

Eine Lehrkraft darf nicht eigenmächtig eine digitale Lernplattform, einen Messenger-Dienst oder ein Videokonferenzsystem zur Nutzung mit Schülerinnen und Schülern einführen, sondern muss dies zuvor der Schulleitung zur Genehmigung vorlegen.

Verarbeitung im Auftrag eines Verantwortlichen – Art. 28 DS-GVO „Auftragsverarbeiter“

Sobald die Schule eine Schulsoftware als „Verantwortlicher“ einsetzt, bedeutet das in der Regel, dass die Schule die Verarbeitung nicht selbst durchführt, sondern sich eines Auftragsverarbeiters bedienen muss. Dies ist bei fast allen im Internet angebotenen Softwareprodukten der Fall. Nimmt man hier als Beispiel die **nicht** gemäß den Bestimmungen der DS-GVO datenschutzgerecht gestalteten Software „Padlet“, so ist zwischen der Schule und der der Fa. Padlet bzw. Wallwisher Inc., San Francisco ein Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DS-GVO abzuschließen. Der Auftragsverarbeiter Wallwisher Inc. müsste hinreichende Garantien dafür bieten, dass die Verarbeitung im Einklang mit allen Anforderungen der DS-GVO steht (vgl. Art. 28 Abs. 1 DS-GVO).
In dem Vertrag ist auszuschließen, dass eine Übertragung von Nutzerdaten an Dritte erfolgt, sofern diese nicht zwingend für den Betrieb der Plattform erforderlich ist. Der Abschluss eines individuellen Auftragsverarbeitungsvertrags zwischen der Schule und „Padlet“ ist aber nicht vorgesehen. Vielmehr muss der Nutzer (die Schule) den festgelegten Geschäftsbedingungen von „Padlet“ zustimmen.

Link zum Muster eines Auftragsverarbeitungsvertrags unter:
https://www.tlfdi.de/mam/tlfdi/themen/tlfdi_formulierungshilfe_fur_auftragsverarbeitungsvertraege.pdf
Ausführliche Hinweise zur Auftragsdatenverarbeitung allgemein sind nachzulesen unter:
https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_13_auftragsverarbeitung.pdf

Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung (festgelegte, eindeutige und für legitime Zwecke erhobene Daten dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden
- Datenminimierung
- Speicherbegrenzung (Daten nur so lange speichern, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.)
- Integrität und Vertraulichkeit (Es muss eine angemessene Sicherheit der personenbezogenen Daten gewährleistet werden durch geeignete technische und organisatorische Maßnahmen.)

Artikel 6 DS-GVO

Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung **eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer **Aufgabe** erforderlich, **die im öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich**, sofern nicht die Interessen** oder Grundrechte und Grundfreiheiten der **betroffenen Person**, die den Schutz personenbezogener Daten erfordern**, überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um **ein Kind** handelt.

*2 Unterabsatz 1: **Buchstabe f** gilt **nicht für die von Behörden** in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.*

Artikel 6 DS-GVO

Rechtmäßigkeit der Verarbeitung

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 **Buchstaben c und e** wird festgelegt durch

a) Unionsrecht oder

b) das **Recht der Mitgliedstaaten**, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

Spezialrechtliche Normen für die Schule

Die **DS-GVO** regelt als EU-Verordnung den Schutz natürlicher Daten bei der Verarbeitung personenbezogener Daten. Nach EG 7 ist das Ziel der DS-GVO einen soliden, kohärenten und klar durchsetzbaren Rechtsrahmen in der EU zu schaffen. Die DS-GVO enthält aber zahlreiche **Öffnungsklauseln – hier: Art. 6 Abs. 1 Satz 1 lit. c) und e) i. V. m. Abs. 3 DS-GVO -** , die den EU-Mitgliedstaaten die Möglichkeit geben, mit der eigenen Gesetzgebung die Vorschriften zu ergänzen, selbst zu regeln, zu konkretisieren, zu modifizieren usw.
Dies sind sowohl das **Bundesdatenschutzgesetz** (für Bundesbehörden und nicht-öffentliche Stellen) als auch die Landesdatenschutzgesetze, in Thüringen das **Thüringer Datenschutzgesetz** (für alle öffentliche Stellen in Thüringen, z. B. TMBJS, ThILLM, staatliche Schulen usw.)

Spezielles Gesetz im Schulbereich ist das **Thüringer Schulgesetz** und die hierzu erlassene **Thüringer Schulordnung** und die **Thüringer Allgemeine Schulordnung für die berufsbildenden Schulen. Darüber hinaus muss das** Lehrpersonal die erlassenen Verwaltungsvorschriften beachten.

§ 57 ThürSchulG

- Abs. 1: Verarbeitung/Nutzung personenbezogener Daten nur bei Erforderlichkeit für den mit den Aufgaben verbundenen Zweck
  - Es ist nicht Aufgabe der Schule, Kinderdaten in die USA zu transferieren.
- Abs. 2: Verpflichtung, Schüler, Lehrer, Eltern etc. , die erforderlichen Angaben zu machen
- Abs. 3: Regelungen zur Schulgesundheitspflege
- Abs. 4: Regelungen zum Kinderschutz
- Abs. 5: Wissenschaftliche Forschungsvorhaben
- Abs. 6: Regelungen zu Vergleichsuntersuchungen
- Abs. 7: Regelungen zu Umfragen ohne Auskunftspflicht
- Abs. 8: Verordnungsermächtigung
- Abs. 9: Für alles, was im ThürSchulG nicht geregelt ist, gilt die DS-GVO i. V. m. dem ThürDSG

§ 136 ThürSchulO

- Abs. 1: Daten, die bei der Aufnahme eines Schülers in die Schule erhoben werden sollen
- Abs. 2: Verpflichtung der Eltern, Veränderungen der Daten der Schule mitzuteilen
- Abs. 3: Inhalt des Schülerbogens
- Abs. 4: Inhalt von Klassen- und Kursbüchern
- Abs. 5: Bei der automatisierten und nicht automatisierten Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen.
- Abs. 6: Bei der Nutzung von Privatgeräten haben Lehrer geeignete technische und organisatorische Maßnahmen zu treffen (Individuelle Genehmigung des Schulleiters gemäß Verwaltungsvorschrift des TKM vom 5. Mai 2000 ist erforderlich.)

§ 136 ThürSchulO -Fortsetzung-

Abs. 7: In Krisen- oder Notfällen können das Schulamt und das Ministerium die dort genannten Daten im automatisierten Verfahren abrufen

Abs. 8: Automatisiert und nicht automatisiert verarbeitete personenbezogene Daten sind ein Jahr, nachdem der Schüler die Schule verlassen hat, einzuschränken.

Abs. 9: Aufbewahrungsfristen von schulischen Unterlagen (siehe auch FAQ-Liste des TMBJS unter 5.3)

Abs. 10: Löschungs- und Archivierungsfristen nach Ablauf der Aufbewahrungsfristen

Fazit: **Es gibt keine gesetzliche Befugnis der Schule zum Einsatz digitaler Tools, mit denen eine Verarbeitung personenbezogener Daten erfolgt. Daher ist nach derzeitiger Rechtslage eine Einwilligung der Eltern/Schüler erforderlich und ausreichend, wenn die übrigen Voraussetzungen der DS-GVO eingehalten werden.**

Die Einwilligung und der Unterschied zu den Informationen nach Art. 13 DS-GVO

Die Definition einer **„Einwilligung“** ist in Art. 4 Nr. 11 DS-GVO und die Bedingungen für die Einwilligung in Art.7 DS-GVO geregelt.

Zusammenfassend ist die Einwilligung

- eine unmissverständliche Willensbekundung
- für einen bestimmten Fall und
- in informierter Weise, dass die betroffene Person mit der Verarbeitung der sie betreffenden Daten einverstanden ist.
- Der Verantwortliche muss dies nachweisen können.
- Die Einwilligung muss verständlich, in leicht zugänglicher Form und in klarer und einfachen Sprache erfolgen.
- Die betroffene Person kann ihre Einwilligung jederzeit widerrufen. Hiervon ist sie vor Abgabe der Einwilligung in Kenntnis zu setzen.

Ein Formularbeispiel einer Einwilligung ist nachzulesen unter: https://www.tlfdi.de/mam/tlfdi/datenschutz/anwendungsbeispiel_einwilligung_.pdf

Eine ausführliche Darstellung der Einwilligung gemäß der DS-GVO ist abzurufen unter: https://www.tlfdi.de/mam/tlfdi/themen/kurzpapier_20.pdf

Einwilligung
(Art. 6 Abs. 1 Satz 1 Buchstabe a), Art. 7 DS-GVO, EG 42):

Informierte Einwilligung

Der Betroffene soll vor der Einwilligung wissen:

- Wer darf die Daten nutzen,
- welche Daten werden genutzt,
- zu welchem Zweck,
- ob die Daten an Dritte übermittelt werden, an wen und zu welchem (anderen) Zweck,
- wie lange die Nutzung dauert.

Die Einwilligung und der Unterschied zu den Informationen nach Art. 13 DS-GVO

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche nach Art. 13 DS-GVO der betroffenen Person zu diesem Zeitpunkt Folgendes mit:

- Namen und Kontaktdaten des Verantwortlichen
- Ggf. Kontaktdaten des Datenschutzbeauftragten
- Zwecke und Rechtsgrundlage der Verarbeitung
- Ggf. die Empfänger der personenbezogenen Daten
- Ggf. die Absicht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln (Angemessenheitsbeschlusses der Kommission oder einen Verweis auf geeignete oder angemessene Garantien)
- Dauer der Speicherung
- Information über Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruchsrecht, Recht auf Datenübertragbarkeit
- Widerrufsrecht im Falle einer Einwilligung

Die Einwilligung und der Unterschied zu Informationen nach Art. 13 DS-GVO Fortsetzung…

- Information über Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit
- Widerrufsrecht im Falle einer Einwilligung
- Beschwerderecht bei einer Aufsichtsbehörde
- Information darüber, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für Vertragsabschluss erforderlich ist und welche möglichen Folgen die Nichtbereitstellung hätte
- Bestehen einer automatisierten Entscheidungsfindung und Informationen hierüber sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung auf die betroffene Person
- Sollen die Daten für einen anderen Zweck weiterverarbeitet werden, so muss die betroffenen Person hierüber informiert werden und alle Informationen über diesen anderen Zweck erhalten

Die Einwilligung und der Unterschied zu Informationen nach Art. 13 DS-GVO

Die Informationspflicht nach Art. 13 DS-GVO besteht also **immer**, wenn personenbezogene Daten vom Verantwortlichen bei der betroffenen Person erhoben werden. Dabei ist es unerheblich, auf welcher Rechtsgrundlage die Daten erhoben werden. Daher ist auch im Falle einer Einwilligung neben der Einholung dieser Einwilligung **zusätzlich** die betroffene Person - wie zuvor aufgeführt - nach Art. 13 DS-GVO zu informieren.

Hinweise zu den Informationen zur Erhebung von personenbezogenen Daten nach Art. 13 und 14 DS-GVO: https://www.tlfdi.de/mam/tlfdi/datenschutz/hinweise_zu_den_informationen.pdf

Wichtiger Hinweis: Mit einer Einwilligung kann nur eine (sonst fehlende) Rechtsgrundlage ersetzt werden. Hingegen kann eine Einwilligung nicht Verstöße gegen die Datensicherheit (Art. 32 DS-GVO) legitimieren.

Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände
und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO

Diese Maßnahmen schließen ggf. unter anderem Folgendes ein:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO

Fortsetzung:

- Risiken berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
- Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Weitere Regelungen speziell zur Datensicherheit finden sich auch in den Artikeln 5 Abs. 1 lit. f), 24, 25, 36 DS-GVO.

Nähere Ausführung sind nachzulesen unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/sicherheit-der-verarbeitung-nach-dsgvo/ und ausführlich mit weiteren Verweisen unter https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/zawas/praxisnahe-hilfe-zum-technisch-organisatorischen-datenschutz-173395.html

Das Urteil des Europäischen Gerichtshofs „Schrems II“ - Rechtssache C-311/18 und „Standardvertragsklauseln“

Der EuGH hat in seiner Entscheidung „Schrems II“ (C-311/18) am 16. Juli 2020 den Beschluss der europäischen Kommission zum angemessenen Datenschutzniveau auf der Grundlage des Abkommens **EU-US „Privacy Shield“** als weitere Rechtsgrundlagen für Datenübermittlungen in die USA für **ungültig** erklärt. Damit dürfen personenbezogene Daten in aller Regel nicht mehr wie bisher auf dieser Grundlage in die USA übermittelt werden. Als Begründung führt das EuGH u. a. an, dass aufgrund der in den USA bestehenden Überwachungsmaßnahmen massenhafte Sammlungen personenbezogener Daten ohne klare Beschränkungen erfolgen. Außerdem haben die europäischen Bürgerinnen und Bürger keine Möglichkeit, diese Überwachungsmaßnahmen von US Behörden gerichtlich überprüfen zu lassen. Zwar existieren noch die Standardvertragsklauseln, in denen geregelt werden kann, dass auch in Drittländern das europäische Datenschutzniveau gewahrt wird. Die aus der Sicht der DS-GVO unzulässigen Zugriffsrechte können aber auch mit den Standardvertragsklauseln nicht verhindert werden.

Damit verstößt eine Datenübermittlung in die USA u. a. gegen Art. 32 DS-GVO.
Wichtig: Eine Einwilligung durch die Eltern der Schülerinnen und Schüler stellt kein rechtswirksames Mittel für eine zulässige Nutzung des Verfahrens dar, weil der Verantwortliche (die Schule) die Einhaltung der technisch-organisatorischen Regelungen der DS-GVO (Art. 25, Art 32 DS-GVO) gewährleisten können müsste, was er jedoch nicht kann. Deshalb ist eine Einwilligung in diesem Bereich unwirksam und keine Option.

Mögliche Online-Lernplattformen im Schulunterricht

Mit **„Moodle“,** mit dem virtuelle Kursräume zur Verfügung stehen, die mit Inhalt gefüllt werden können und auch Lernaktivitäten gestaltet werden können. Moodle wird von mehreren Schulen genutzt und teilweise vom Schulträger angeboten.

In drei Bundesländern (Bremen, Schleswig-Holstein, Mecklenburg-Vorpommern) läuft als Landeslösung die Lernplattform **„itslearning“**. Nach Kenntnis des TLfDI kann dieses Lernmanagementsystem ebenfalls datenschutzgerecht betrieben werden.

Kursorisch geprüft hat der TLfDI auch die Schulsoftware **„EduPage“**. Die Software stellt viele Funktionen zur Verfügung, angefangen von der Verwaltung von Schulverwaltungsdaten bis zur Durchführung von Unterricht. Solange ausschließlich die e-Learning Funktionen, also der pädagogische Teil (erstellen von Lernkarten, Online-Hausaufgaben, Kontrollieren von Hausaufgaben usw.) genutzt wird, scheint der Einsatz von „EduPage“ aus datenschutzrechtlicher Sicht zulässig zu sein. Es dürfen mit der Software aber nicht gleichzeitig Schulverwaltungsdaten z. B. auf dem gleichen privaten DV-Gerät einer Lehrkraft verarbeitet werden.

Als kleine Lernplattform ist die „**Anton-App“** für die 1. bis zur 10. Klasse zu bezeichnen. Diese wurde vom TLfDI ebenfalls mit den zur Verfügung stehenden „Bordmitteln“ aus datenschutzrechtlicher Sicht geprüft. Zur Anmeldung an der App kann ein Pseudonym verwendet werden. Nach der Datenschutzerklärung werden entstehende Daten nicht an Dritte weitergegeben und es werden auch keine Drittbibliotheken von Facebook, Google oder Amazon genutzt. Der Serverstandort ist Deutschland.

Anforderungen an Videokonferenzsysteme im häuslichen Lernen

Schulen, die die Thüringer Schulcloud nutzen, steht auch das Videokonferenzsystem **„BigBlueButton“** zur Verfügung. Da BigBlueButton wie die TSC auf deutschen Servern gehostet wird, kann dieses für Unterrichtszwecke genutzt werden.

Ein weiteres Open-Source Webkonferenzsystem ist **„Jitsi Meet“.** Gegen eine Nutzung von Jitsi Meet sieht der TLfDI ebenfalls keine durchdringenden Bedenken.

Mit einigen Einschränkungen, aber noch datenschutzrechtlich vertretbar, können Schulen auch auf „**Cisco Webex“** zurückgreifen, wenn es in eigenen Rechenzentren oder über die Telekom oder über Bechtle läuft. Cisco Webex als Online-Dienst kann aus datenschutzrechtlicher Sicht nicht empfohlen werden. In der Cisco Online-Datenschutzrichtlinie wird noch immer auf das EU-US-Privacy Shield verwiesen, obwohl dieses vom EuGH (siehe dort die Folie) für ungültig erklärt wurde. Andere Garantien zur Einhaltung der DS-GVO sind nicht enthalten.

Auch für die Videokonferenzsysteme gilt derzeit, US-amerikanische Produkte aufmerksam daraufhin zu prüfen, ob die Einhaltung der DS-GVO garantiert werden kann!

Eine Liste zur datenschutzrechtlichen Bewertung verschiedener Videokonferenzsysteme hat die Berliner Beauftragte für datenschutz und Informationsfreiheit veröffentlicht: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

Eine Orientierungshilfe Videokonferenzsysteme kann abgerufen werden unter: https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-videokonferenzsysteme_final.pdf und die passende Checkliste als Entscheidungshilfe unter: https://www.tlfdi.de/mam/tlfdi/datenschutz/video/20201111_checkliste_oh_videokonferenzsysteme-1.pdf
Zum häuslichen Lernen wird auch auf die Handreichung „Häusliches Lernen“ des TMBJS hingewiesen, zu der der TLfDI zugearbeitet hat: https://bildung.thueringen.de/bildung/haeusliches-lernen/handreichung

Anforderungen an Messenger-Dienste im häuslichen Lernen und für schulische Zwecke

Zunächst ist darauf hinzuweisen, dass mit der Einführung der dienstlichen E-Mail-Adressen für die Thüringer Lehrkräfte im Schuljahr 2019/2020 das Land eine Möglichkeit zur schulischen Kommunikation der Lehrkräfte mit Schüler*innen und Eltern sowie der Lehrkräfte untereinander geschaffen hat, die die Nutzung von Messenger-Diensten überflüssig machen sollen. Hierfür wurde vom TMBJS eine Dienstanweisung erlassen und eine Handreichung zur Einrichtung des E-Mail-Accounts erstellt. Viele weitere Fragen werden in der FAQ-Liste des TMBJS unter 10. beantwortet.
https://bildung.thueringen.de/schule/medien/datenschutz-in-schulen

Eine Nutzung des weit verbreiteten Messenger-Dienstes „WhatsApp“ wird aus datenschutzrechtlicher Sicht für eine schulische Nutzung ausgeschlossen. Die Gründe sind schon oft genannt worden: Abgleich der Kontaktlisten auf den Smartphones, Verarbeitung aller Metadaten der Kommunikation (wer mit wem, wann, wie lange kommuniziert hat und die Weitergabe der Daten an Facebook). In diesem Sinne auch AG Bad Hersfeld, Urteil v. 15.05.2017(Az. F120/17), das zudem klarstellt, dass sich deliktisch verhält, wer die personenbezogenen Daten aus der Telefonliste an WhatsApp=Facebook übermittelt.

Messenger, denen datenschutzrechtlich nur wenige Bedenken begegnen, sind „Textsecure“, „Chatsecure“, „Threema Work Education“ sowie „Schul.Cloud / Stashcat“. Zumindest mit letzterem Verfahren sollen keine sensible Daten im Sinne von Art. 9 DS-GVO versendet werden.

„Bei Kinderdaten hört der Spaß auf“: Datenschützer droht Lehrern mit Strafe

News4teachers, 10. Juni 2020

Art. 83 DS-GVO
Allgemeine Bedingungen für die Verhängung von Geldbußen

1. Jede Aufsichtsbehörde **stellt sicher**, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** ist.

2. Geldbußen **werden** je nach den Umständen des Einzelfalls **zusätzlich** zu oder **anstelle** von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i **verhängt**. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

→

Art. 83 DS-GVO
Allgemeine Bedingungen für die Verhängung von Geldbußen

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

→

Art. 83 DS-GVO
Allgemeine Bedingungen für die Verhängung von Geldbußen

Geldbußen gegen Behörden (Schulen) dürfen nicht verhängt werden.: § 61 Abs. 4 Thüringer Datenschutzgesetz (ThürDSG).

ABER gegen Mitarbeiter:

- wenn sie personenbezogene Daten als Verantwortliche für eigene Zwecke verarbeiten, etwa für private Informationen an Dritte (sog. Exzess),
- nach § 61 ThürDSG bei Datenschutzverstößen.

§ 61 ThürDSG

Ordnungswidrigkeiten und Strafbestimmungen

(1) Ordnungswidrig handelt, wer entgegen den Bestimmungen der Verordnung (EU) 2016/679 , dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten solche Daten

1. erhebt, speichert, verändert, übermittelt oder nutzt,
2. zum Abruf mittels automatisierten Verfahrens bereithält,
3. abruft oder sich oder einem anderen aus Dateien verschafft oder
4. sonst verarbeitet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Ebenso kann mit Geldbuße bis zu fünfzigtausend Euro belegt werden, wer die Übermittlung von personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht.

(4) Gegen öffentliche Stellen nach § 2 Abs. 1 und 2 werden keine Geldbußen verhängt, es sei denn, es handelt sich um öffentliche Stellen, die am Wettbewerb im Sinne des § 26 teilnehmen.

(5) [1] Wer bei einer Handlung nach den Absätzen 1 und 3 gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. [2] Die Tat wird nur auf Antrag verfolgt. [3] Antragsberechtigt sind die betroffene Person und der Landesbeauftragte für den Datenschutz.

(6) Der Landesbeauftragte für den Datenschutz ist Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten in der Fassung vom 19. Februar 1987 (BGBl. I S. 602) in der jeweils geltenden Fassung.

Probleme:

1. Findet das Opportunitätsprinzip des § 47 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) Anwendung, wonach es im pflichtgemäßen Ermessen der Aufsichtsbehörde liegt, das Verfahren einzustellen?

   Nach herrschender Meinung nicht, da Erwägungsgrund 148 Satz 2 DS-GVO besagt, dass von einer Geldbuße nur abgesehen werden darf im Falle eines geringen Verstoßes oder wenn das Bußgeld besonders belasten würde. Es muss also festgestellt werden, ob ein Verstoß vorliegt.

2. Beide Augen zudrücken und Schulleitungen, Lehrerinnen und Lehrer datenschutzrechtlich weiter wurschteln lassen?
   - nicht erforderlich, da rechtmäßige Alternativen zur Verfügung stehen.
   - Thüringen: ca. 50 Hinweise an alle Schulen zu nicht nutzbarer/nutzbarer Software: Online-Lernplattform, Videokonferenzsystemen, Messengerdiensten.
   - Thüringen: regelmäßige Videokonferenzen mit allen Schulleitungen zu aktuellen Online-Unterrichts-Problemen: gute Nachfrage, gute Rückmeldungen, inzwischen sachlicher und zielorientierter Diskurs.
   - Hinweise der Berliner LfDI:
   https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

3. Rolle des Thüringer Ministerium für Bildung, Jugend und Sport:
   - Schulleitungen als datenschutzrechtliche Verantwortliche?
   - Aufgabe von Pädagogen, Software zu beurteilen?
   - Stärkere Verantwortung von Schulämtern und Schulverwaltungsämtern sowie des Ministeriums?

→

Probleme:

4. Digital-Pakt
   - Abruf der Mittel (noch) nicht für Tablets und Software, sondern für WLAN-Anbindung?

5. Große Player im Schulunterricht?
   - WhatsApp (≙ Facebook)
   - Verstoß der Nutzer gegen Datenschutzrecht, weil sie als Verantwortliche Kontaktdaten von Personen aus ihrer Kontaktliste an WhatsApp/Facebook übermitteln, ohne dass eine Einwilligung der Betroffenen hierfür vorliegt (AG Bad Hersfeld vom 15.05.2017, Az. F120/17).
   - Irische Datenschutzbehörde:
     225 Millionen Bußgeld wegen fehlender Transparenz bei der Weitergabe von personenbezogenen Daten: https://www.tagesschau.de/wirtschaft/whatsapp-irland-millionenstrafe-101.html
     Rekordstrafe gegen WhatsApp, 2. September 2021, tagesschau.de
   - YouTube:
   - Pressemitteilung des TLfDI: „YouTube im Unterricht? https://www.tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen_2021/210330_PM_YouTube_in_der_Schule.pdf
   - Problem:
     - YouTube verfolgt Nutzeraktivitäten und speist diese in das Analyseframework von Google,
     - Nutzeranalyse ist kein schulischer Zweck (Schule aber Verantwortlicher),
     - damit auch nicht über eine Einwilligung für Schule zu legitimieren,
     - Alternativen wie Dailymotion.com (Frankreich), Vimeo.com (USA) und ähnlich große Angebote haben gleiches Problem,
     - einzig mögliche Lösung (bisher): schuleigene Geräte ohne Schüler- & Lehrerbezug (d.h. Cookie-Löschung, wechselnde Nutzer, Privatmodus des Browsers usw.).

- Microsoft
- Im Gespräch mit der Datenschutzkonferenz (DSK).
- Verlagerung der Clouds nach Europa: Zugriff amerikanischer Dienste – CLOUD Act (Clarifying Lawful Overseas Use of Data Act)
- Undurchsichtig: Auswertung von Meta-Daten durch “Watson”: Welche Daten werden wie zu welchen Zwecken ausgewertet?

- Google
- Alternativen: MetaGer.de , duckduckgo.com, www.startpage.com

6. Von der Staatssekretärin beauftragtes Gutachten der TU Ilmenau (Prof. Dr. Jens Wolling) von 2018 zur Ketzerei des TLfDI, dass das Schulfach „Medienkunde“ ein Geisterfach sei. Ergebnisse:
   - Medienkunde wird „defizitär“ unterrichtet
   - Lehrerfortbildung – Medienkompetenz „defizitär“ – inzwischen verbessert,
   - Lehrerausbildung – Medienkompetenz: (-)
   - Fundstelle:

https://www.db-thueringen.de/servlets/MCRFileNodeServlet/dbt_derivate_00041138/ilm1-2018100036.pdf

7. Neues Fach “Medienkunde”:
   - Verpflichtend, prüfungsrelevant.
   - Müssen hierfür die Anteile anderer Fächer gekürzt werden oder müssen Zeitanteile durch Kürzung der Ferien gewonnen werden?

8. Zertifikate:
   Nach Art. 42 Abs. 1 DS-GVO werden Zertifikate **nicht** für **Produkte**, sondern für **konkrete Datenverarbeitungsvorgänge** ausgestellt. Diese Lücke sollte schnellstens zugunsten von Unternehmen, Schulleitungen usw. geschlossen werden, damit auf zertifizierte Produkte zurückgegriffen werden kann.

Wie geht es weiter?

1. Alternative Betriebssysteme wie Linux (Open-Source-Anwendung) nutzen.

2. Datenaufsichtsbehörden zu Leistungsbehörden machen.

3. Sachverstand Externer einbinden, um Lücken zu schließen

   - bei der Umsetzung des Faches “Medienkunde” mit IT-Inhalten,
   - in der Lehrerfortbildung,
   - in der Lehrerausbildung.

4. Anders denken:
   Nur weil privat Vielen der Schutz der eigenen Daten und von Daten Dritter gleichgültig ist und das Datenschutzrecht außer Acht gelassen wird, muss es an der (Hoch-) Schule nicht genauso zugehen. Viel mehr muss für die Sinnhaftigkeit der DS-GVO sensibilisiert warden. Wenn Realität und Recht nicht übereinstimmen, sollte man etwas ändern: die Realität oder das Recht.

5. “Zertifizierung” von Software, ohne gegen die DS-GVO zu verstoßen.

6. Koalition der Willigen:

Lehrerinnen und Lehrer, Schülerinnen- und Schülervertretungen, Verlage, KMK, BDA, Bitcom, Bündnis für Bildung, Softwarehersteller, Datenschutzbeauftragte etc., sollten Konzepte, Orientierungshilfen (OH) entwickeln für:

- die länderübergreifende Nutzung von digitalen Lehr-/Lernmitteln,
- die Vorgaben für Schulbuchverlage,
- die Vorgaben für ein Pflichtfach „Medienkunde“,
- die Vorgaben der Lehrerinnen- und Lehrerausbildung und -fortbildung,
- die Vorgaben für „Medienkunde“ bereits in Kindertagesstätten.

Gute Praxis: Kooperation HPI, LfD, etc. zur Erstellung einer Schulcloud -> Thüringen Cloud

- OH-Krankenhaus-Informationssysteme (KIS), Kooperation von Medizinern, ITlern und LfD – heute Standard, der stets weiterentwickelt wird.

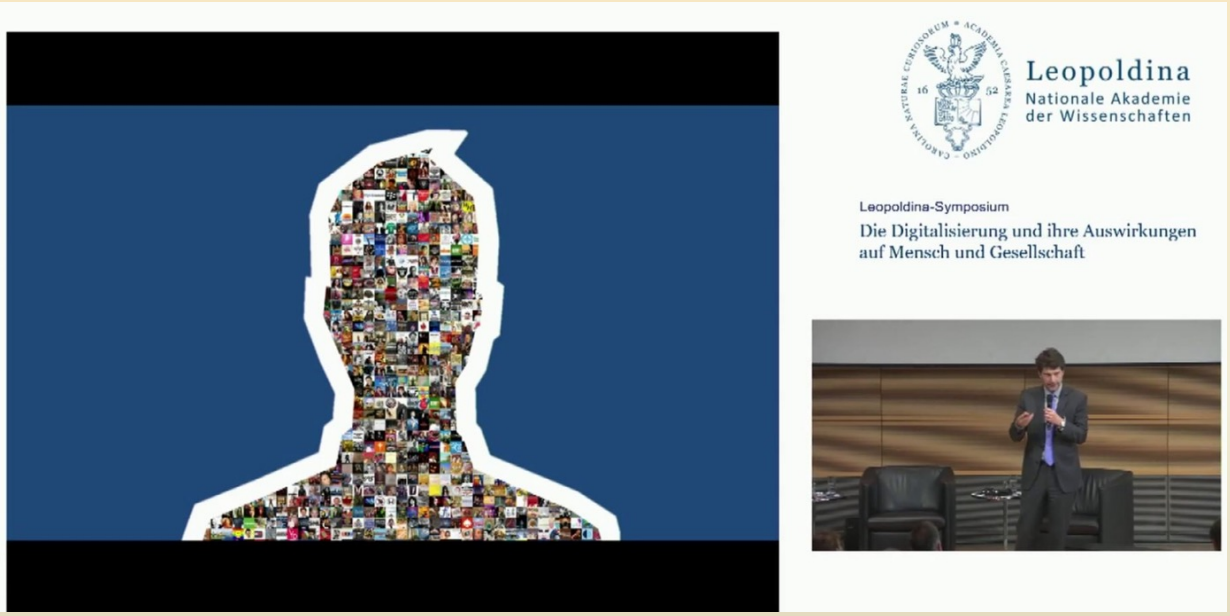
7. Verbesserung der

- Lehrerinnen- und Lehrerfortbildung: Mehr Zeitanteile für Fortbildung – Anreizsysteme (z.B. Beförderungen)
- Lehrerinnen- und Lehrerausbildung; Problem: Unabhängigkeit von Wissensinhalt und Forschung: finanzpolitische Einwirkungsmöglichkeiten, Schaffung von bestimmten Lehrstühlen (wie in einigen Bundesländern bereits geschehen).

8. Nochmal anders denken:

Nur weil Lehrerinnen und Lehrer (pandemiebedingt) gelernt haben, welche Software DS-GVO-konform arbeitet und wie man mit ihr umgeht, bedeutet das **nicht**, dass sie **rechtlich** wissen, warum das so ist und **technisch** wissen, was da passiert. Das sollten Schülerinnen und Schüler im digitalen Zeitalter aber schon kennen – also auch die Lehrerinnen und Lehrer.

Leopoldina-Symposium
Die Digitalisierung und ihre Auswirkung auf Mensch und Gesellschaft
Prof. Michal Kosinski, Stanford Graduate School (USA)



Offene Fragen zu „Datenschutz und Schule“?

Danke für die Aufmerksamkeit

Bildnachweise

Fotolia:
© fotomek - Runder Tisch - fotolia.com
© Robert Kneschke - Dozent hilft Studierenden - fotolia.com
Fotolia_53470038© eyetronic - fotolia.com
© eyetronic -Adler BfG - fotolia.com
© Speedfighter - Thuringia coat of arms - fotolia.com

Andere Quellen:
Bildschirmfoto aus Video „The Power of Big Data and Psychographics“; Concordia, New York
Textauszug, Foto aus „Datenschutz-Berater, Heft 12, S. 255 und 256,
Handelsblatt Fachmedien GmbH, Düsseldorf

Alle weiteren Grafiken und Bilder: Pixabay CC0 Public Domain sowie TLfDI