Medienbildung braucht technische und rechtliche Bildung

> *Die einen sagen so.*
> *Die anderen sagen so.*
> *Und dann ändert sich das alles auch noch dauernd.*

2022-01 dirk.weller@zsl-rstue.de

Motivation / Wie kam es zu dieser Präsentation? Im Moodle-Kursraum einer KG des ZSL Gemeinschaftskunde fand sich ein Dokument eines Tübinger Pädagogen mit dem Titel „Positivliste digitaler Tools“. Die dort aufgeführten Einschätzungen waren für mich nicht nachvollziehbar, der Autor mir nicht als mit Datenschutzthemen vertraut bekannt, eine Suche nach Hinweise auf technische Kompetenzen des Autors verlief ergebnislos: es handelte sich um einen empirisch arbeitenden Unterrichtsforscher.
Der Autor nannte weder seine Untersuchungsmethode noch legte er Kriterien für seine Einschätzung offen noch gab dieser konkrete Handlungsanweisungen zu seinen Urteilen wie „Datenschutz: unbedenklich“ oder „Datenschutz: eingeschränkt“.

Das Zitat ist im Grunde richtig! Aber die Lösung des Problems ist nicht „Wurstigkeit“ oder blindes Vertrauen in irgendjemand.

These: Unmöglichkeit von Medienbildung im 21. Jh ohne grundlegendes technisches und rechtliches Verständnis der involvierten Materie

Zu mir: Redaktionsleitung und somit Beschäftigung mit datenschutzrechtlichen Fragen im Berufsalltag; grundlegendes technisches Verständis durch LPIC-2 u.a. Zertifizierungen, Fortbildungen (u.a. Netzwerksicherheit), Pflege einer Serverinfrastruktur mit > 25 Rootservern, eigener „Spieltrieb“, Fortbildung bDSB

Zur Präsentation:
1 rechtlichen Hintergrund
2 technische Werkzeuge, mit denen „Normalsterbliche“ Dienste so überprüfen können, dass eine Einschätzung deren Einsatzes im Unterricht bezüglich „ist möglich / nicht möglich“ bzw. „Aufwand lohnt sich / nicht“ besser möglich ist
3 GA, in der die Werkzeuge selbst ausprobiert werden können

BP2016: Leitperspektive Medienbildung

Die Entwicklung unserer Gesellschaft zu einer Mediengesellschaft macht Medienbildung zu einem wichtigen Bestandteil allgemeiner Bildung. Ziel von Medienbildung ist es, Kinder und Jugendliche so zu stärken, dass sie den neuen Anforderungen sowie den Herausforderungen dieser Mediengesellschaft selbstbewusst und mit dafür erforderlichen Fähigkeiten begegnen können. Dazu gehören eine **sinnvolle, reflektierte und verantwortungsbewusste Nutzung** der Medien sowie eine **überlegte Auswah**l aus der Medienvielfalt in Schule und Alltag. Um diese Kompetenzen zu vermitteln, muss Medienbildung fächerintegriert unterrichtet werden. Die grundlegenden Felder der Medienbildung sind Information, Kommunikation, Präsentation, Produktion, Analyse, Reflexion, Mediengesellschaft, Jugendmedienschutz, **Persönlichkeits-**, Urheber-, Lizenz**recht** und **Datenschutz**.

Die Verankerung der Leitperspektive im Bildungsplan wird durch folgende Begriffe konkretisiert:

- Mediengesellschaft
- Medienanalyse
- Information und Wissen
- Kommunikation und Kooperation
- Produktion und Präsentation
- Jugendmedienschutz
- **Informationelle Selbstbestimmung und Datenschutz**
- **Informationstechnische Grundlagen**

Quelle: http://www.bildungsplaene-bw.de/,Lde/LS/BP2016BW/ALLG/LP/MB

… das seh also nicht nur ich so ...

BP 2016: pbK (Auswahl)

2.3 Handlungskompetenz

8. bei der Nutzung von Medien die Grundsätze des **Datenschutzes** und der **informationellen Selbstbestimmung** beachten

2.4 Methodenkompetenz

1. selbstständig **Recherchetechniken** nutzen und auch an außerschulischen Lernorten (zum Beispiel Parlament, Rathaus, Gericht) Informationen gewinnen und verarbeiten

2. die gewonnenen Informationen quellenkritisch hinterfragen und dabei die Zuverlässigkeit der unterschiedlichen Medien einschätzen

4. Informationen aus **Rechtstexten** entnehmen (zum Beispiel Allgemeine Erklärung der Menschenrechte, UN-Charta, UN-Kinderrechtskonvention, Grundgesetz, Jugendschutzgesetz, Schulgesetz, SMV-Verordnung)

Bezugspunkte in den pbK gibt es viele – hier nur ein paar offensichtliche ...

BP2016: ibK (Auswahl an Anküpfungspunkten)

3.1.2.1 Recht

(4) Prinzipien des Rechtsstaats charakterisieren (Garantie der Grundrechte …)

3.1.2.2 Grundrechte

(4) an einem vorgegebenen Fallbeispiel einen Grundrechtskonflikt analysieren

3.1.3.5. Kontrolle politischer Herrschaft

(1) die Kontrolle politischer Herrschaft durch Medien erläutern (zum Beispiel investigativer Journalismus)

3.1.3.6 Problemlösefähigkeit pol.Sys.

(1) anhand eines aktuellen politischen Konflikts (zum Beispiel ... Digitalisierung ...) eine Fallstudie erstellen

3.1.4.2 EU

(1) erläutern, wie Entscheidungen der EU das tägliche Leben der EU-Bürger beeinflussen

(5) an einem vorgegebenem Fallbeispiel eine länderübergreifende Herausforderung innerhalb der EU anhand des Politikzyklus analysieren und Lösungsmöglichkeiten erörtern (zum Beispiel … Digitalisierung ...)

3.1.2.1

z.B. Datenschutz als Grundrecht

3.1.2.2

z.B. Datenschutz versus Bildung?
z.B. Digitalisierung first – Bedenken second?

3.1.3.5

z.B. politische Videos von Rezo

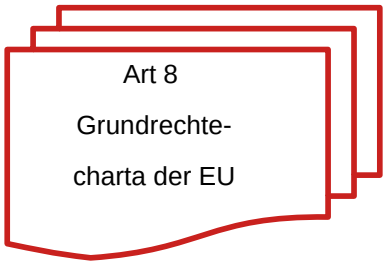
3.1.3.6

z.B. Digitale Souveränität als Technologiesouveränität versus locked-in by MS
WD 3 - 3000 – 102/21; WD 3 - 3000 – 181/20 usw usw usw
https://www.datenschutz-mv.de/presse/?id=168438

3.1.4.2

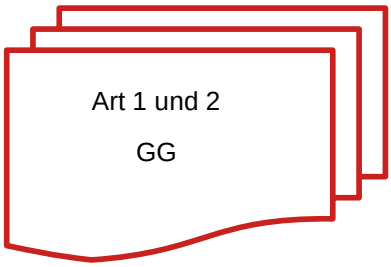
z.B. EU-DSGVO
z.B. EuGH, Urteil vom 6. Oktober 2015, C-362/14, (Schrems I), Aufhebung von Safe Harbor
z.B. EuGH, Urteil vom 16. Juli 2020, C-311/18, (Schrems II), Aufhebung von EU-US Privacy Shield.

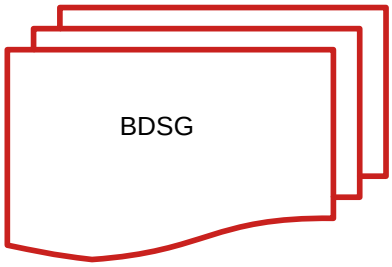
Rechtsgrundlagen

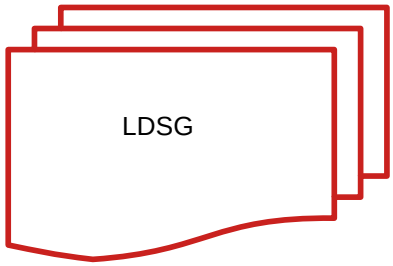


Art. 8 Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese **Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden**. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.







Insgesamt hohe Komplexität des Themengebietes

- viele Rechtsnormen
- auf unterschiedlichen Ebenen
- zusätzlich Gerichtsurteile
- vielfältige Einschätzungen von Datenschutzbehörden
- stellenweise umstrittene bzw. nicht letztinstanzlich geklärte Fragestellungen

Einigkeit bezüglich: Datenschutz = Grundrecht / Individualrecht, in das nur auf Grund von Gesetzen und gegenüber dem Betroffenen transparent eingegriffen werden kann

= viele Pflichten für den Eingreifenden

BVerfGE 65 vom 15.12.1983 „Volkszählungsurteil“

> Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs. 1 in Verbindung mit GG Art 1 Abs. 1 umfaßt. **Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.**

BVerfGE 65 Leitsatz 1 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html, Hervorhebung dw

Individualrecht - so auch BVerfG:

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

Begründungskern BVerfGE 65 vom 15.12.1983 „Volkszählungsurteil“

> **Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende 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. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

BVerfGE 56 RN 146 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html, Hervorhebung dw

Erneut diskutiert insbes. „nach Snowden“ unter dem Begriff „chilling effects“ – vgl. hierzu auch

Rechtssprechung und CE:
https://www.telemedicus.info/was-sagt-die-rechtsprechung-zu-chilling-effects/

Empirischer Nachweis der Wirkung von chilling effects in:

Penney, Jonathon, Chilling Effects: Online Surveillance and Wikipedia Use (2016). Berkeley Technology Law Journal, Vol. 31, No. 1, p. 117, 2016, Available at SSRN: https://ssrn.com/abstract=2769645
via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

Aktualisierung der Argumentation (mit Anklängen an die in GemK vertraute Auseinandersetzung zu Elisabeth Noelle-Neumanns Schweigespirale):

Penney, Jonathon, Understanding Chilling Effects (May 28, 2021). 106 Minnesota Law Review ___ (2022, Forthcoming), Available at SSRN: https://ssrn.com/abstract=3855619
via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855619

und dort insbes. Seite 171 ff zur Auseinandersetzung mit Slansky und Posner

PEN zu chilling effects durch staatliche Überwachung:
https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf

Definition „Personenbezogene Daten“ (pbD)

Art 4 EU-DSGVO 1

alle Informationen, die sich auf eine **identifizierte oder identifizierbare** natürliche Person (im Folgenden „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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

PbD dienen der direkten oder indirekten Identifikation eines konkreten Menschen

PbD konkret

- Allgemeine Personendaten (Name, Geburtsdatum, Alter, Geburtsort, Postanschrift, E-Mail-Adresse, Telefonnummer etc)
- Kennnummern (Sozialversicherungs-, SteuerID-, Personalausweisnummer etc)
- Bankdaten (Kontonummer, Kreditinformationen, Kontostand, Geldinstitut etc)
- **Online-Daten (IP-Adresse, Cookies, GPS-Standortdaten etc)**
- Physische Merkmale (Geschlecht, Haut- / Haar- / Augenfarbe, Statur, Kleidergröße, Bilder etc)
- Besitzmerkmale (Fahrzeug-, Immobilieneigentum, Grundbucheinträge, KFZ-Kennzeichen, MAC, IMEI etc)
- Kundendaten (Benutzerprofile, Bestellungen, Adressedaten, Bankverbindung etc)
- **Werturteile** (Schul-, Studienabschluss, Noten, Arbeitszeugnisse, Diplome, Zertifikate etc)
- ...

Zum *ETC* bei Onlinedaten und Besitzmerkmalen – ein erster Einblick:

https://www.zendas.de/service/browserdaten.html

Fingerprinting Demos:

https://privacycheck.sec.lrz.de/index.html#fingerprintingCollection

Auch dynamische IPs (z.B. Internetanschluss zu Hause) sind pbD!
EuGH Urteil vom 19.10.2016 – C-582/14
https://curia.europa.eu/juris/document/document.jsf;?text=&docid=184668&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=3164186
BGH Urteil vom 16.05.2017 – VI ZR 135/13
https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=78741&pos=0&anz=1

Ergebnis des Tests mit Zendas: Browser übermitteln viele Daten, die zur Identifikation genutzt werden können. Dabei sind das noch nicht alle Informationen – bei Zendas fehlend sind u.a. installierte Schriftarten, Add-ons, ...

Dazu kommen diverse Fingerprinting Technologien zur Identifikation trotz evtl. eingesetzter Spoofs für die klassischen Verfahren: vgl. dazu die vielen Möglichkeiten hier https://privacycheck.sec.lrz.de/index.html

Hinweis: Da Cookies und Fingerprinting zunehmend unter Druck geraten, überlegt sich die Branche inzwischen neue Techniken. Mehr dazu hier: https://www.kuketz-blog.de/tracking-durch-identitaetsprovider/

Problematisch ist hier IMHO v.a. die seitenübergreifend mögliche Verfolgung eines Benutzers, weil Diensteanbieter auf die „immergleichen“ Trackingdiensleister zugreifen.

Literaturhinweise:
https://www.ted.com/talks/gary_kovacs_tracking_our_online_trackers (2012!)
https://dl.acm.org/doi/10.1145/2872427.2883028#d27490504e1
https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users

Rechtsgrundlagen im Alltag

https://it.kultus-bw.de/
https://www.baden-wuerttemberg.datenschutz.de/

DSFA: DatenSchutzFolgeAbschätzung | DViA: DatenVerarbeitung im Auftrag | VV: Verzeichnis der Verarbeitungstätigkeiten | TOM: technisch organisatorische Maßnahmen

(6) **Die Lehrkräfte tragen** im Rahmen der in Grundgesetz, Verfassung des Landes Baden-Württemberg und § 1 dieses Gesetzes niedergelegten Erziehungsziele und der Bildungspläne sowie der übrigen für sie geltenden Vorschriften und Anordnungen **die** unmittelbare pädagogische **Verantwortung** für die Erziehung und Bildung der Schüler. **Sie entscheiden in diesem Rahmen auch über den Einsatz informationstechnisch gestützter Systeme.**

zwischen EU-DSGVO einerseits und der sich aus der Vielfalt gesetzlicher Bestimmungen und Rechtsverordnungen ergebenden Anforderungen / Verpflichtungen (wie DSFA etc. pp. … von denen „Normalsterbliche“ meist nicht einmal gehört haben) andererseits

Verständliche Reaktion: Kann das bitte mal einer übersetzen in möglichst einfache und (bei gutem Willen) verständliche Handlungsleitlinien?

Rechtsfolgen für Schulen (zusammenfassende Auszüge)

- §1 SchG (Erziehungs- und Bildungsauftrag)
  - Legitim – Geeignet – Erforderlich – Angemessen
- Verarbeitung der Daten
  - Lokal = meist unproblematischer
  - Dienstleister = Vertrag zur DViA nötig
- Übermittlungszwecke
  - Werbezwecke = immer unzulässig
  - Zweckänderung nur in Ausnahmefällen (z.B. Gefahrenabwehr, Straftaten)
- Besondere Datenkategorien (vgl. Art 9 EU-DSGVO)
  - Ethnie (inkl. Sprache im Haushalt), Religionszugehörigkeit, biometrische Daten, **politische Meinungen, religiöse oder philosophische Überzeugungen**, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Sexualleben, ...
  - hier: Rechtsvorschrift oder ausdrückliche Einwilligung!
- Schule (!) muss sicherstellen
  - Anbieter hat technische und organisatorische Datenschutzmaßnahmen nach § 3 LDSG (BW) getroffen
  - Rechte der Betroffenen sind gewahrt – vgl. Art 12 – 23 EU-DSGVO
    - transparente Information zu Verantwortlichen, Rechtsgrundlagen, Speicherort und -dauer, ...
    - Recht auf Berichtigung, Löschung, Sperrung, ...

„**Die Speicherung personenbezogener Daten in einer ‚Cloud' beziehungsweise die dienstliche Nutzung von sogenannten ‚Cloud-Diensten' ist unzulässig**, **wenn** die Voraussetzungen nach Artikel 28 EU-DSGVO nicht vorliegen oder wenn der **Dienstleister oder die genutzten Server sich außerhalb des räumlichen Anwendungsbereichs der EU-DSGVO befinden.**" (RN 1.14.2)

vgl. https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen und dort insbesondere AZ 13-0557.0/106 vom 04. Juli 2019

Keine Schnellschlüsse! Z.B.

lokale DV: meist (!) unproblematischer – aber abhängig von der Art der verarbeiteten Daten, dem Betriebssystem, der konkreten Software und deren Verhalten, dem Speicherort der Daten, evtl. des konkret verwendeten Verschlüsselungsverfahrens etc. pp. Deswegen: Gilt **nicht** für Tablets und Smartphones!

Rubrik „besondere Datenkategorien" macht klar, dass wir in GemK (aber auch in anderen Fächern, die persönliche Stellungnahmen von S einfordern) bei den Operatoren auf Niveau III ein Problem haben!

Vgl. zum Standort des Anbieters auch:

„Eine Verarbeitung personenbezogener Daten von Schulen außerhalb des Geltungsbereichs der EU-DSGVO sollte grundsätzlich unterbleiben und ist nur im Ausnahmefall (z.B. Auslandsschule) mit Zustimmung des Kultusministeriums zulässig."

https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Cloudbasierte_Dienste

Exkurs: Privatwirtschaftliche DV und staatlicher Zugriff

Die Speicherung personenbezogener Daten in einer ‚Cloud' beziehungsweise die dienstliche Nutzung von sogenannten ‚Cloud-Diensten' ist unzulässig, wenn die Voraussetzungen nach Artikel 28 EU-DSGVO nicht vorliegen oder wenn **der Dienstleister oder die genutzten Server sich außerhalb des räumlichen Anwendungsbereichs der EU-DSGVO befinden**.

AZ 13-0557.0/106 vom 04. Juli 2019 RN 1.14.2

§ 2713. Required preservation and disclosure of communications and records

A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or **disclose the contents** of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, **regardless of whether such communication, record, or other information is located within or outside of the United States**.

https://www.justice.gov/dag/cloudact

Warum diese Beschränkung in den KM Papieren auf die EU?

Teil der Begründung liegt im US-Cloud-Act: Zugriff der US-Behörden auf Daten von US-Unternehmen auch im Ausland

Hier: Konflikt zwischen staatlicher Souveränität und Schutzverpflichtung (Grundrechte) auf mehreren Ebenen: BaWü – BRD – EU – USA | Datenschutz – Schutz vor Kriminalität | schriftlichen Zusicherungen – konkretem Verhalten

Hinzu kommt sicherlich auch eine durch Nicht-EU-Dienste / -Dienstleister erschwerte Durchsetzung individueller Rechte vor Gericht.

Zusammenfassend der LfDI hier:
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf

Aufgrund der Befugnisse der US-Geheimdienste und der Rechtslage in den USA kann ein angemessenes staatliches Datenschutz-Niveau (Art. 45 DS-GVO) nicht sichergestellt werden (u. a.):

- *Section 702 des Foreign Intelligence Surveillance Act (FISA) sieht keine Beschränkungen der Überwachungsmaßnahmen der Geheimdienste und keine Garantien für Nicht-US-Bürger vor,*
- *Presidential Policy Directive 28 (PPD-28) gibt Betroffenen keine wirksamen Rechtsbehelfe gegen Maßnahmen der US-Behörden und sieht keine Schranken für die Sicherstellung verhältnismäßiger Maßnahmen vor,*
- *der im Privacy Shield vorgesehene Ombudsmann hat keine genügende Unabhängigkeit von der Exekutive; er kann keine bindenden Anordnungen gegenüber den Geheimdiensten treffen*

Auswahl zentraler Prüfkriterien

konkrete Datenkategorie immer mitdenken!

- Nutzung ohne Anmeldung / Pseudonymisierung / Anonymisierung
- keine für Zielerreichung unnötige Erfassung von
  - IP, IMEI, UDID, IMSI, MAC
  - Standortdaten
  - biometrische Daten
  - Nutzungsdaten (wer, wann)
  - Inhaltsdaten etc.
- keine unnötigen Zugriffe auf
  - Kalender, Adressbuch, Anruflisten (insbes. Apps)
  - Bilder, Dateien …
- Verschlüsselung
  - der Daten auf dem Gerät / Server
  - der Internetverbindung (z.B. SSL, VPN)
  - techn. entscheidend: Wer hat die Schlüssel?
- Backup
  - konkrete Angaben zu Technik und Ort
  - Löschung gewährleistet
- AGB
  - keine Änderung ohne Information der Nutzer
  - transparente Beteiligung von Dritten (Unterbeauftragung)
  - keine Werbung etc.
- Dienstleister selbst
  - Sachkenntnis (Pannenstatistik!)
  - BSI Zertifizierung, ISO 27001, ISO 27018 …
  - RZ-, Unternehmenssitz EU / EWR
  - Verständlichkeit der Nutzungsbedingung, Datenschutzseite
  - Konkretion der Angaben
- konkreter Vertrag zur DviA / TOMs

Sicherstellung der Weisungsbefugnis der Schule

Erstellt auf Basis von 53-6534.440/423

Ist gewährleistet, dass …

Wie wird dies gewährleistet?
Wie kann die Schule die Einhaltung kontrollieren?

Zur Pannenstatistik siehe auch:
https://www.netzwelt.de/news/175645-microsoft-datenleck-ueber-250-millionen-kundendaten-netz-offen-zugaenglich.html

Versuch einer Graduierung

von sachkundigem Landesbeamten betriebene, mindestens transportverschlüsselte Dienste (nur FOSS) auf eigener Hardware in eigenem RZ	in ISO 27001 zertifiziertem EU-RZ von einem ISO 27018 zertifiziertem Dienstleister, mit dem ein Vertrag zur DViA besteht, mindestens transportverschlüsselt betriebene (FOSS und auch proprietäre) Dienste	in nicht-zertifizierten RZ außerhalb der EU von nicht-zertifizierten Unternehmen mit Firmensitz außerhalb der EU, das besonderen Auskunftspflichten seiner Regierung gegenüber unterliegt, betriebene proprietäre Dienste, bei der Transportverschlüsselung nicht / nicht vollständig gewährleistet ist

Grün: Idealfall
Gelb: formal OK - materiell Kontrollprobleme (deswegen ISO Zertifizierung!)
Rot: offensichtliches NoGo

… und zwischen den einzelnen Farbfeldern ist viel Platz für alle nur erdenklichen Zwischentöne … jeweils in Abhängigkeit von den konkret verarbeiteten Datenkategorien.

Transportverschlüsselungsprobleme ergeben sich auch beim Einsatz von CDN: hier wird a) die Verbindung intern nicht verschlüsselt oder b) der CDN Dienstleister hat die Schlüssel. In beiden Fällen hat er Vollzugriff auf den Datenstrom = Auftragsdatenverarbeitung

Bei der Kategorisierung „Idealfall“ folge ich weitgehend

Ernst, Christian; Der Grundsatz digitaler Souveränität. Eine Untersuchung zur Zulässigkeit des Einbindens privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung. in: Schriften zum Öffentlichen Recht (SÖR), Band 1426; 2020 via https://directory.doabooks.org/handle/20.500.12854/48965

und gehe dabei davon aus, dass im Falle von SuS-Daten (Minderjährige!) eine besondere Schutzpflicht des Staates immer besteht, also out-sourcing nur dann ausnahmsweise möglich wäre, wenn der Staat die Leistung nachweislich nicht selbst erbringen kann, Kontrollmöglichkeiten trotzdem voll umfänglich bestehen, besondere Schutzmaßnahmen getroffen werden können (Wer hat die Schlüssel?) und die Datenkategorien dies zulassen (vgl. „besondere Datenkategeorien“ in GemK).

Umsetzung

- Anmeldung?
- Anbieter selbst
  - unterliegt der DSGVO? VDViA möglich?
  - Impressum
- Einverständnis für Cookies?
- Hinweise auf Zugriffe Dritter
  - Analyse Webseite – z.B. eingebundene Scripte, Cookies
  - Datenschutzseite des Anbieters
- Hilfsmittel für eine oberflächliche (!) Analyse
  - Analyse des HTML Quelltextes
    - https://webbkoll.dataskydd.net/de/
    - https://noscript.net/ und / oder https://addons.mozilla.org/de/firefox/addon/ublock-origin/
  - https://checkgoogleanalytics.psi.uni-bamberg.de/
  - https://reports.exodus-privacy.eu.org/de/ (für Android-Apps)
  - Besser wäre: Netzwerkanalyse mit Burp Suite, mitmproxy, Wireshark etc. - vgl https://www.kuketz-blog.de/mitmproxy-app-verkehr-mitschneiden/

Keine der so gesammelten Informationen gibt Auskunft über das, was beim Dienstleister intern geschieht!

Einsatz wird im folgenden gezeigt …

Weitere Tools:

https://privacyscore.org/ (Uni Bamberg)

Padlet (Webseite)

- Basisinformationen

  https://webbkoll.dataskydd.net/de/results?url=http%3A%2F%2Fpadlet.com

  - IP Adresse
  - Cookies versus Cookie Banner
  - weitere Drittanfragen
- Google Analytics:

  https://checkgoogleanalytics.psi.uni-bamberg.de/scan/result/?url=http%3A//padlet.com

Ohne Login:

- CDN Cloudflare Inc
- 16 first-party Cookies, stellenweise bis 2072 haltbar
- keine Cookie-Informationen erhalten / keine Zustimmung eingeholt
- 8 US-Drittdienste rudderlabs, alexametrics, cloudflareinsights, googletagmanager
- googleanalytics USA ohne IP Anonymisierung

Webbkollseite besprechen!

Cookies
Cookies können Benutzer identifizieren – auch über die Grenze von Seiten hinweg
deren Verfallsdaten sind ebenso interessant wie deren Inhalte (Wert)
Drittanbieter-Cookies sollten einen besonders hellhörig machen – aber auch Cookies die schon in ihrem Namen Drittanbieter referenzieren
Nebenwirkungen können mit einem sauber konfiguriertem Browser in den meisten Fällen aufgefangen werden – SuS haben eine solchen fast nie.
Gab es eine Information des Anbieters über Cookies (Cookie Banner)?
Drittanfragen
Auf der Webseite eingebundene Scripte etc. pp. von Dritten, die dann ebenfalls Anwenderdaten erhalten.
Ein Klick auf die jeweils angebene IP erlaubt deren grobe geographische Einordnung.
CDN in den URLS bedeutet in den meisten Fällen den Einsatz eines Content Delivery Networks, was dann wiederum bedeuten kann, dass die Transportverschlüsselung intern (zwischen den Servern des CND und dem Anbieter) nicht mehr besteht bzw. einfach aufgemacht werden kann (z.B. bei Passworteingaben etc. interessant)
Unterscheiden sich die hier angegebenen IPs von der IP des Anbieters? Dann nutzt dieser evtl. nur für Teile seines Angebots ein CDN.
IP-Adresse
Die über die IP abrufbaren Geoinformationen sind der interessante Teil.

Die Datenschutzseite des Anbieters sollte über alle Aspekte aufklären!

Padlet: Ein Blick in den HTML Quelltext der Seite

```
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=G-4M6WGE55N0"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());
  gtag('config', 'G-4M6WGE55N0', {
    'anonymize_ip': true,
    'user_id': $pepinUser.userId,
  });
  gtag('set', 'user_properties', {
    'registration_status': $pepinUser.userRegistration,
    'plan_name': $pepinUser.userPlanName,
    'days_since_first_visit': $pepinUser.userAge,
  })
</script>
```

Aus einer Mail der Uni Bamberg:

Bei padlet.com handelt es sich um eine nicht korrekte Aktivierung der IP-Anonymisierungsfunktion. Korrekt müsste es in der Konfiguration im JavaScript-Quelltext „anonymizeIp“ heißen.
Bei Google Analytics werden alle weiteren Parameter, die nicht bekannt sind, einfach weitergegeben unter ep.* (vermutlich ep = extra parameter).
Würde es beispielsweise wie folgt eingebunden:

```
// [...]
gtag('config', 'G-4M6WGE55N0', {
  'anonymize_ip': true,
  'ichbinunbekannt': true,
  'user_id': $pepinUser.userId,
});
// [...]
```

gäbe es zusätzlich zu „ep.anonymize_ip“ auch noch ein „ep.ichbinunbekannt“ mit dem Wert „true“ in den Request-Parametern. Der Parameter „ep.anonymize_ip“ hat also keine Wirkung: es ist einfach nur ein weiterer – aufgrund der falschen Schreibweise für Google Analytics unbekannter – Parameter.
Falsch ist übrigens auch „anonymizeIP“ (es muss Ip, nicht IP heißen). Bei richtiger Schreibweise wird ein Parameter „aip=1“ (ohne „ep.“ als Prefix) angehängt.

Spielt aber eigentlich keine Rolle mehr, denn GA ist so oder so kritisch zu betrachten:

https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf

Padlet (App)

https://reports.exodus-privacy.eu.org/de/reports/com.wallwisher.Padlet/latest/

- 5 Tracker (alle USA)
  - Branch
  - Google
  - Microsoft
- 26 Berechtigungen
  - Access_Fine_Location
  - Phone_State



2 der 5 Tracker (Google, MS) beziehen sich auf die Analyse von Crash-Daten

3 Tracker (Branch, Google, MS) beziehen sich auf das Sammeln von Nutzungsdaten (Telemetrie)

Das Recht Access_Fine_Location soll – so die Angaben auf der Datenschutzseite der Webseite – nur zur Anwendung kommen, wenn ein Benutzer eine Karte hinzufügt. Ob das auch für die App zutrifft (und wie dies technisch im Detail umgesetzt ist) entzieht sich meiner Kenntnis.

Padlet (Wallwisher, Inc. 981 Mission St San Francisco, CA 94103)

https://legal.padlet.com/privacy

- „**We use Google Analytics' IP anonymization feature** to prevent them from associating your activity with your identity."
- „We work with **many vendors**, service providers, and other partners to help us provide the Service by performing tasks on our behalf. These service providers **may be located inside or outside of the European Economic Area** ("EEA")."
- „Over time, Padlet may grow and reorganize. We may **share your personal information with affiliates such as a parent company, subsidiaries, joint venture partners or other companies that we control or that are under common control with us**, in which case we will require those companies to agree to use your personal information in a way that is **consistent** with this Policy."
- „We may amend this Privacy Policy from time to time. In case of **major changes**, we will notify users by email addresses provided to us."

Angaben zu GA IP Anonymisierung sind nach Test mit Uni Bamberg Tool und Rücksprache mit den dortigen Entwicklern (1.2022) schlicht falsch! Das wird in der „subprocessor list" auch in sich widersprüchlich erwähnt (vgl. Spaltenkopf mit dem Zellinhalt)

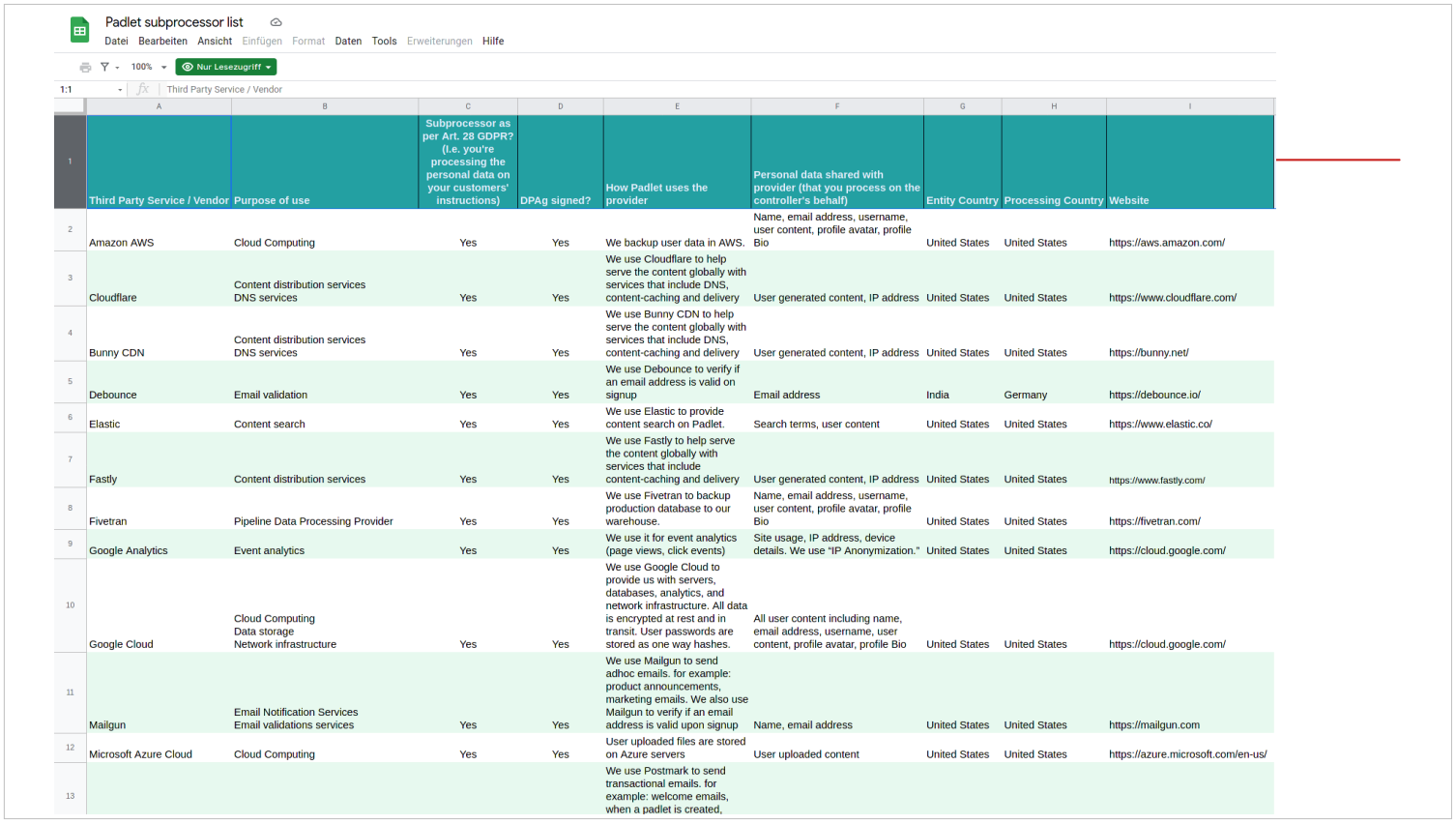
Zusammenarbeit mit weitere Nicht-EU Partnern (konkret z.B. aus Indien), die nicht genau benannt sind (zu unbestimmt).

Unklare Rechtsbegriffe aus dem angelsächsischem Recht. Was genau bedeutet „that are under common control with us" oder was ist im in diesem Rechtsraum „Konsistenz" von Verträgen? Identisch kann kaum gemeint sein.

„We may amend" steht im Konflikt zum deutschen Vertragsrecht. Benutzer sollen über „major changes" informiert werden, was die Frage aufwirft, was bei einer Vertragsänderung „major" wäre.

Keine Angaben zur Zertifizierung (und kein Freigabe durch KM / LfDI vorliegend)

Verlinkt: Liste an Subunternehmen mit sehr knappen Informationen – als Google Doc. Diese Liste konnte 1.2022 nicht herunter geladen und auch nicht gedruckt werden.



Padlet subprocessor list

Datei Bearbeiten Ansicht Einfügen Format Daten Tools Erweiterungen Hilfe

100% Nur Lesezugriff

1:1 Third Party Service / Vendor

Third Party Service / Vendor	Purpose of use	Subprocessor as per Art. 28 GDPR? (I.e. you're processing the personal data on your customers' instructions)	DPAg signed?	How Padlet uses the provider	Personal data shared with provider (that you process on the controller's behalf)	Entity Country	Processing Country	Website
Amazon AWS	Cloud Computing	Yes	Yes	We backup user data in AWS.	Name, email address, username, user content, profile avatar, profile Bio	United States	United States	https://aws.amazon.com/
Cloudflare	Content distribution services DNS services	Yes	Yes	We use Cloudflare to help serve the content globally with services that include DNS, content-caching and delivery	User generated content, IP address	United States	United States	https://www.cloudflare.com/
Bunny CDN	Content distribution services DNS services	Yes	Yes	We use Bunny CDN to help serve the content globally with services that include DNS, content-caching and delivery	User generated content, IP address	United States	United States	https://bunny.net/
Debounce	Email validation	Yes	Yes	We use Debounce to verify if an email address is valid on signup	Email address	India	Germany	https://debounce.io/
Elastic	Content search	Yes	Yes	We use Elastic to provide content search on Padlet.	Search terms, user content	United States	United States	https://www.elastic.co/
Fastly	Content distribution services	Yes	Yes	We use Fastly to help serve the content globally with services that include content-caching and delivery	User generated content, IP address	United States	United States	https://www.fastly.com/
Fivetran	Pipeline Data Processing Provider	Yes	Yes	We use Fivetran to backup production database to our warehouse.	Name, email address, username, user content, profile avatar, profile Bio	United States	United States	https://fivetran.com/
Google Analytics	Event analytics	Yes	Yes	We use it for event analytics (page views, click events)	Site usage, IP address, device details. We use "IP Anonymization."	United States	United States	https://cloud.google.com/
Google Cloud	Cloud Computing Data storage Network infrastructure	Yes	Yes	We use Google Cloud to provide us with servers, databases, analytics, and network infrastructure. All data is encrypted at rest and in transit. User passwords are stored as one way hashes.	All user content including name, email address, username, user content, profile avatar, profile Bio	United States	United States	https://cloud.google.com/
Mailgun	Email Notification Services Email validations services	Yes	Yes	We use Mailgun to send adhoc emails. for example: product announcements, marketing emails. We also use Mailgun to verify if an email address is valid upon signup	Name, email address	United States	United States	https://mailgun.com
Microsoft Azure Cloud	Cloud Computing	Yes	Yes	User uploaded files are stored on Azure servers	User uploaded content	United States	United States	https://azure.microsoft.com/en-us/
				We use Postmark to send transactional emails. for example: welcome emails, when a padlet is created,				

Stand Screenshot: 06.01.2022
https://docs.google.com/spreadsheets/d/1sJAt34Co7SyJHSwNmm6UsMxlgaJurg0RbPW5NwhFRFk/edit#gid=1979223826

Fehlend scheinen die folgenden Informationen zu sein:
- Rudderlabs (Customer Data Platform? https://rudderstack.com/?)
- Alexametrics (Amazon USA?)
- Serverstandort für Backups (Fivetran USA?)

Lückenhaft scheinen die folgenden Diensleister erwähnt:
- CDNs erhalten beim Userlogin die Möglichkeit, Passwörter mitzulesen. Eine Information wie „We ensure passwords are stored and transferred securely using encryption and salted hashing“ (Datenschutzseite) scheitert in der Umsetzung, wenn das CDN die Schlüssel hat
- der Name „Cloudflare Insights“ verweist auf Analyse- und Telemtrieaufgaben - hier nicht erwähnt
- Speicherung der (aller?) Inhalte auf Google Cloudservern steht so nicht auf der Datenschutzseite (dort „The Service is hosted on servers at a third-party facility, with whom we have a contract providing for enhanced security measures.“)

Telekommunikation-Telemedien-Datenschutz-Gesetz = Änderungen der obigen Einschätzung durch Inkrafttreten des TTDSG am 1.12. 2021 zu erwarten!
Betreiber von Webseiten, aber auch Hersteller von Smartphone-Apps müssen sicherstellen, dass bei der Verarbeitung personenbezogener Daten alle Vorgaben der Datenschutz-Grundverordnung (DSGVO) eingehalten werden.
Die bisherigen Datenschutz-Regelungen des Telemediengesetzes (TMG) können seit Mai 2018 insbesondere auf die Einbindung von Elementen Dritter und webseitenübergreifendes Tracking nicht mehr angewendet werden.

Einsatz von Padlet als LMS?

IMHO

Aber ...

https://imgflip.com/i/608ci9 built on Jake Clark; Be a dick – don't be a dick [C] via https://jake-clark.tumblr.com/post/100946716432

- keine Nutzung als LMS, aber unter den folgenden Voraussetzungen IMHO möglich
  - aus der Schule (nur IP des Schulnetzes nach Außen sichtbar)
  - ohne SuS-Login (also nur für den Abruf von Informationen in einem [mit Passwort geschütztem / öffentlichen] Pad durch S)
  - von Geräten, die keiner Person zugeordnet werden können = keine persönlichen S-Laptops / -Tablets / -Handys (z.B. keine personenbeziehbare UDID, IMEI, MAC …) = auch kein BYOD
  - ohne Verbindung zu weiteren Diensten (z.B. paralleler Login bei Instagram in einem anderen Browsertab oder via App)
  - mit sauber konfiguriertem Firefox als Browser evtl. inklusive weiterer Maßnahmen: DNS over HTTPS im Browser ist aus und DNS Tracking-/Werbe-Filter der Schule vorhanden (DNS Hole), sauber konfiguriertes OS ...

Es mag manchmal voraussetzungsreich sein, aus einem „Geht gar nicht“ ein „Geht doch“ zu machen … wenn es sich lohnt.

Gesamtergebnis

Karikatur von O.Kock:

Eine Kuh steht einem Nashorn (evtl. auch einem Nilpferd mit einem Papphorn auf der Nase?) gegenüber. Das Nashorn sagt: „Vertraue mir! Ich bin ein Einhorn!“

Da es offensichtlich ist, dass das Nashorn kein Einhorn ist, lautet die zentrale Aussage der Karikatur, nicht auf die Behauptungen eines Gegenübers zu vertrauen, sondern „sich selbst ein Bild zu machen“ – also Behauptungen immer kritisch zu prüfen.

Die Karikatur im Kontext der vorangegangenen Ausführungen interpretiert:

- Vertraue nicht den Aussagen Dritter (oder gar Marketingabteilungen)
- recherchiere selbst zum Anbieter
- prüfe mit den Dir zur Verfügung stehenden technischen Mitteln
- entscheide dann, ob Aufwand (z.B. Vertrag zur DViA, Dokumentations- und Prüfpflichten etc. pp.) und unterrichtlicher Nutzen im richtigen Verhältnis zueinander stehen und wie ein datenschutzkonformes Nutzungskonzept aussehen könnte

Hinweis: Es gibt saubere Alternativen zu Padlet.
Diese beginnen bei Wikis, Kanban-Boards, Cryptpads und Etherdads … bis hin zu Moodlekursräumen (die insbesondere beim Einsatz entsprechender Themes auch schnieke aussehen), die dann auch weitaus mehr Funktionalitäten bieten.
Oder, wer es lieber kommerziell und in einem ähnlichen Layout haben will:
https://www.taskcards.de/#/home/start
- Abschluss eines VDViA nicht vergessen!

Verhältnismäßigkeitsprüfung

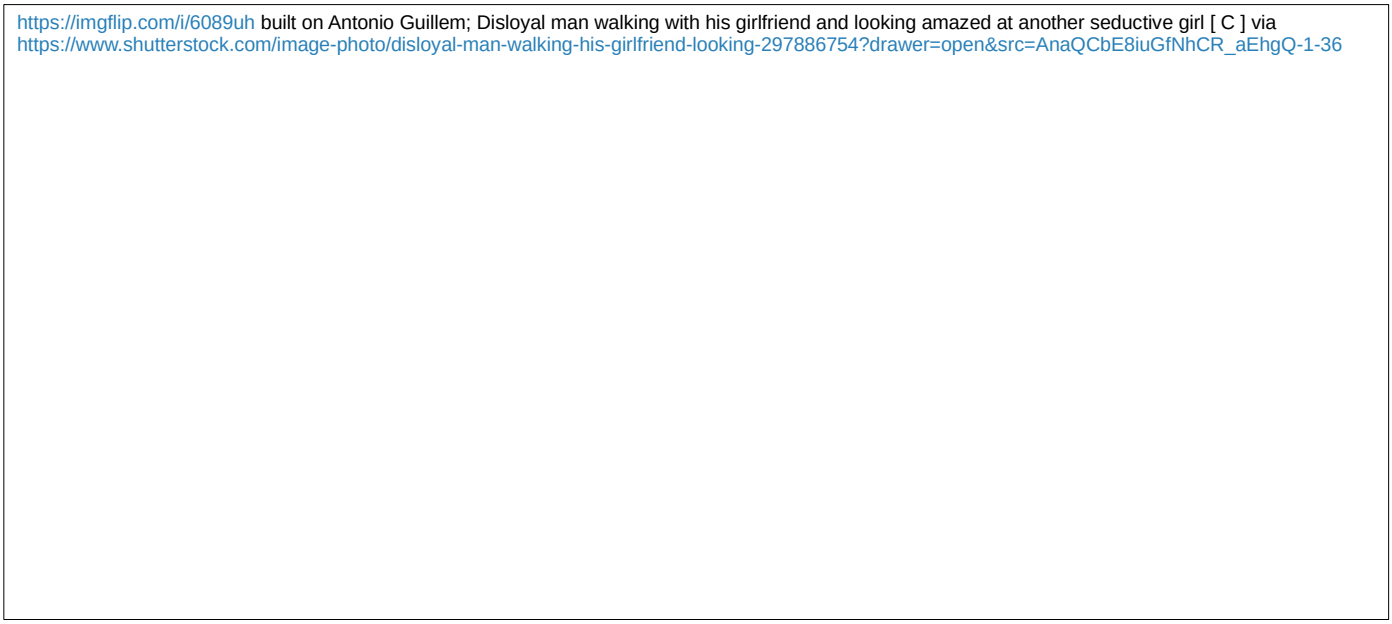
Geeignetheit	Erforderlichkeit	Angemessenheit
Ja	Werkzeuge, die weniger in die Rechte der Betroffenen eingreifen, stehen zur Verfügung.	

Was nicht geeignet ist, kann nicht erforderlich sein. Was nicht erforderlich ist, kann nicht angemessen sein.
Eine Diskussion „Artikel 26 der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen vom 10. Dezember 1948 (Recht auf Bildung) versus Art 8 EU-Grundrechtecharta, Art 1 und 2 GG … Verwaltungsvorschriften des KM (Datenschutz)“ kann deswegen hier unterbleiben.

Wer trotz der vorangegangenen Ausführungen zu anderen Ergebnissen kommen sollte, ist von den umfangreichen Dokumentationspflichten keineswegs entbunden und muss die dienst-/haftungsrechtlichen Fragen selbst klären … und sich selbstverständlich trotzdem an Recht und Gesetz halten.

Geeignetheit: Wenn die Maßnahme die Erreichung des Zwecks kausal bewirkt oder zumindest fördert, ist sie geeignet.
Erforderlichkeit: Die Maßnahme ist erforderlich, wenn kein milderes Mittel gleicher Eignung zur Verfügung steht, genauer: wenn kein anderes Mittel verfügbar ist, das in gleicher (oder sogar besserer) Weise geeignet ist, den Zweck zu erreichen, aber den Betroffenen und die Allgemeinheit weniger belastet.
Angemessenheit: verhältnismäßig im engeren Sinn ist eine Maßnahme nur dann, wenn die Nachteile, die mit der Maßnahme verbunden sind, nicht völlig außer Verhältnis zu den Vorteilen stehen, die sie bewirkt. An dieser Stelle ist eine Abwägung sämtlicher Vor- und Nachteile der Maßnahme vorzunehmen. Dabei sind vor allem verfassungsrechtliche Vorgaben, insbesondere Grundrechte zu berücksichtigen.

Meme dazu?



Hinweis: Auch der für obiges Meme genutzte Memegenerator https://imgflip.com/memegenerator sollte nur unter den für „Padlet“ bereits genannten Bedingungen (aus der Schule, keine personalisierten Geräte, keine parallel bestehenden Logins …) verwendet werden.

Vgl hierzu:

https://webbkoll.dataskydd.net/de/results?url=http%3A%2F%2Fimgflip.com%2Fmemegenerator

Alternativen: Eine einfache Bildbearbeitung / Whiteboard ist meist völlig ausreichend für die Platzierung von Text auf Bild

Zur urheberrechtlichen Seite von Memes vgl.
https://irights.info/artikel/nicht-immer-unversoehnlich-meme-und-urheberrecht/27367

Technische Sichtung und datenschutzrechtliche Einschätzung der Spielvorschläge der LFT-GemK-KG

Gruppen

1) https://www.getbadnews.de
2) https://fakeittomakeit.de/
3) https://unionslabor.de/

Arbeitsaufträge:

1 Überprüfen Sie die Spieleseite mit Hilfe von

- https://webbkoll.dataskydd.net/de/
- https://checkgoogleanalytics.psi.uni-bamberg.de/
- Datenschutzseite, Impressum etc.

2 Beurteilen Sie Einsatzmöglichkeiten aus datenschutztechnischer und -rechtlicher Sicht.

3 Entwerfen Sie ein technisches Szenario für einen datenschutzrechtlich sauberen Einsatz des Spiels.

Ergebnisse aus der GA Phase

Darstellung der Ergebnisse durch die TN, Diskussion

Meine Ergebnisse

getbadnews.de

- kein Login
- Technik: GA mit IP Adressanonymisierung, Drittanbieter: G Tagmanager, Eigencookie 2 Jahre, DigitalOcean LLC (USA)
- kein Impressum, keine Datenschutzseite
- Seite erhebt in integrierter Umfrage pbD

unionslabor.de

- Pseudonym nutzbar
- Technik: kein GA, Drittanbieter unpkg.com, Google, Typekit, Youtube, Eigencookie 1 Jahr, A100 ROW GmbH auf Amazon Cloud Servern (USA)
- Impressum verweist auf GbR, Datenschutzseite erwähnt Drittdienste nicht, Zusendung von „Spielergebnissen“ möglich (Email = pbD)

fakeittomakeit.de

- kein Login
- Technik: GA ohne IP Anonymisierung, Eigencookie 2 Jahre, Drittanbieter: Google, LinkedIn (MS), A2 Hosting Inc (USA)
- Impressum BzfpB, Datenschutzseite unvollständig und nicht DSGVO konform

Mein Ergebnis für alle 3: Nutzung in der Schule, kein BYOD

Stand 2021-01-04

Hinweis zur Umfrage in getbadnews:

- Altersgruppe
- Geschlecht
- Bildungsstand
- Positionierung im politischen Spektrum
- ...

Aussprache

Weiter ...

… mit einer inhaltlich-didaktischen Betrachtung der Spiele.

Literatur

Literatur

- https://it.kultus-bw.de/IT,Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen
- https://www.baden-wuerttemberg.datenschutz.de/
- https://lehrerfortbildung-bw.de/st_recht/

Blogs, Medien, NGOs mit Datenschutzschwerpunkt

- https://www.kuketz-blog.de/
- https://privacy-handbuch.de/
- https://digitalcourage.de/
- https://netzpolitik.org/
- https://www.ccc.de/de/topics
- https://noyb.eu/de

Tools für Oberflächenanalyse

- https://webbkoll.dataskydd.net/de/
- https://reports.exodus-privacy.eu.org/de/
- https://checkgoogleanalytics.psi.uni-bamberg.de/
- https://noscript.net/
- https://addons.mozilla.org/de/firefox/addon/ublock-origin/
- https://www.northdata.de/

Tools für tiefergehende Analysen

- https://www.wireshark.org/
- https://portswigger.net/burp
- https://mitmproxy.org/
- https://www.kali.org/

Weitere Literatur ist jeweils auf den Notizenseiten direkt angegeben.