

FÄCHERÜBERGREIFENDES PROJEKT OBERSTUFE: MEDIENBILDUNG IM KONTEXT VON BIG DATA

MEDIENBILDUNG, INFORMATIK, DARSTELLENDES SPIEL, KUNST,
DEUTSCH, POLITIK UND WIRTSCHAFT

Teil 1

Big Data

versus DSGVO

- Spiegel-Mining von David Kriesel
- Was ist Big Data?
- Datenfeatures
- Daten verknüpfen
- Data Analyse und Data Abuse
- Was ist die DSGVO?
- Was bedeutet die DSGVO für Unternehmen und uns?
- Wo werden Daten im Umfeld gesammelt?
- Welche Arten von Daten werden in meinem Umfeld gesammelt?
- Positionierungsspiel

Teil 2

DSGVO

im Kontext

- Gruppenarbeiten zu einem Kontextthema
 - **Podcast**-Erstellung und Aufnahme
 - **Kurzfilm**-Erstellung mit Szenenbeschreibung/Drehbuch
 - Entwurf eines "Schon gewusst?"-**Flyers**
 - Design einer passenden **Social-Media-Kampagne**
- Auseinandersetzung mit BigData
- Verknüpfung des Kontexts mit DSGVO
- Erstellen des Produkts und Beleuchtung der DSGVO-Konformität

Kontextthemen

Schatten-
profile

Kranken-
kassen &
Wearables

Personal-
isierte
Werbung

Deep Fakes

ChatBots
und Alexa,
Siri & Co

Predictive
Policing

Smarte
Fahrzeuge

Smart
Home und
IoT

Teil 3

Auswertung

und Reflexion

- S-Produkte werden vorgestellt
- Was hat der Kontext mit BigData/der DSGVO zu tun?
- BigData/DSGVO in unserem Alltag
- Reflexion im Umgang mit den eigenen Daten
- Vergleich eines Positionierungsspiels zu gewissen Thesen
- Warum sollte man Daten schützen?
- Aussprache über Datenschutz und Eigenverantwortlichkeit im Umgang mit Daten
- Apell an sensiblen Umgang mit Daten
- Anregung der Selbstreflexion durch schülernahen Einblick in die Gesetzeslage und den Umgang mit den eigenen Daten durch Dritte

Big Data versus DSGVO

I. Idee, Zielsetzung und Konzeption

a) Was hat Sie zu der Durchführung dieses Medienprojekts bewegt?

Die rasante Entwicklung digitaler Technologien und die wachsende Relevanz von Big-Data-Anwendungen haben in den letzten Jahren zu einem tiefgreifenden Wandel der Informations- und Kommunikationskultur geführt. Immer mehr Lebensbereiche werden von Datenanalysen und Algorithmen geprägt, während gleichzeitig die Privatsphäre von Nutzerinnen und Nutzern bedroht sein kann. Vor diesem Hintergrund ist das Projekt „**Big Data vs. DSGVO**“ entstanden, um Schülerinnen und Schülern die komplexen Zusammenhänge von Datenverarbeitung und Datenschutz **praxisnah** und **fächerübergreifend** zu vermitteln.

Besonders die **europäische Datenschutz-Grundverordnung (DSGVO)** erfordert ein Bewusstsein dafür, wie mit personenbezogenen Daten umzugehen ist. Da Kinder und Jugendliche heute tagtäglich Online-Dienste nutzen, ist es essenziell, ihnen bereits in der Schule einen verantwortungsvollen und zugleich kritischen Umgang mit Daten näherzubringen. Zusätzlich war ein entscheidender Beweggrund die wachsende Bedeutung von **sozialen Netzwerken** in politischen Prozessen. Beispiele wie der US-Wahlkampf 2015/2016, bei dem Desinformationskampagnen über Facebook und Co. aufgedeckt wurden, oder die jüngeren Manipulationsvorwürfe im Zusammenhang mit den rumänischen Wahlen verdeutlichen, wie stark Social-Media-Plattformen das Wahlverhalten beeinflussen können. Daher erschien es zwingend notwendig, Jugendlichen Kompetenzen in der Erkennung von Fake News und der reflektierten Nutzung digitaler Medien zu vermitteln.

b) Welche Ziele bzw. Kompetenzen wollen Sie den Kindern/Jugendlichen vermitteln?

Das Hauptziel von „Big Data vs. DSGVO“ besteht darin, Jugendliche für die **technischen**, **rechtlichen** und **ethischen** Aspekte der Datenverarbeitung zu sensibilisieren und sie gleichzeitig in die Lage zu versetzen, multimediale Inhalte eigenständig zu erstellen. Konkret werden folgende Kompetenzen gefördert:

1. **Technische Kompetenz:** Ein grundlegendes Verständnis von Big Data, Algorithmen und Künstlicher Intelligenz, um datengetriebene Prozesse einzuordnen.
2. **Rechtliche Kompetenz:** Kenntnis der DSGVO, ihrer Anwendungsbereiche und der individuellen Datenschutzrechte.
3. **Reflexionsfähigkeit:** Kritischer Umgang mit der eigenen Datennutzung und der Datenverarbeitung durch Dritte, insbesondere im schulischen Alltag oder bei Social-Media-Plattformen.
4. **Medienproduktion:** Praktische Fertigkeiten in der Produktion von Podcasts, Kurzvideos, Infolyern und Social-Media-Beiträgen.
5. **Politische Mündigkeit:** Fähigkeit, Falschmeldungen zu erkennen, manipulative Techniken zu durchschauen und eine eigenständige Meinungsbildung zu entwickeln.
6. **Teamarbeit und Planung:** Durch das Arbeiten in Kleingruppen und das Einhalten von Deadlines stärken die Jugendlichen ihre Projektmanagement- und Kommunikationsfähigkeiten.

c) Welche Projektbausteine haben Sie geplant?

„Big Data vs. DSGVO“ gliedert sich in mehrere Bausteine, die jeweils unterschiedliche Schwerpunkte setzen und den Jugendlichen einen ganzheitlichen Zugang zum Thema Medienkompetenz ermöglichen:

- **Theoretische Einführung:** Grundlagen zu Big Data, Datenschutz und der DSGVO, um ein solides Fundament an Wissen zu schaffen.
- **Podcast-Produktion:** Von der Recherche über das Formulieren von Interviewfragen bis hin zur Aufnahme und dem Schnitt lernen die Jugendlichen, Inhalte auditiv aufzubereiten.
- **Kurzvideo-Erstellung:** Entwicklung eines Drehbuchs, Kameraführung, Beleuchtung und Videoschnitt vermitteln filmische Gestaltungsmöglichkeiten.
- **Infolyer-Gestaltung:** Hier geht es um die prägnante Reduktion komplexer Daten- und Datenschutzthemen auf das Wesentliche sowie eine ansprechende visuelle Umsetzung.
- **Social-Media-Kampagnen:** Planung und Umsetzung von Beiträgen, die sich gezielt an Zielgruppen richten und dabei datenschutzrechtliche Aspekte berücksichtigen.
- **Einsatz von KI-Tools (z. B. ChatGPT):** Die Jugendlichen lernen, KI-generierte Inhalte kritisch zu analysieren und ethische Fragestellungen zu reflektieren.
- **Politische Medienbildung:** Das Erkennen von Fake News und Desinformation sowie das Verständnis, wie Social Media das Wahlverhalten und die öffentliche Meinungsbildung beeinflusst, bilden einen eigenen Baustein.

Durch diese abwechslungsreichen Komponenten schaffen wir ein Lernsetting, das Theorie und Praxis verzahnt und die Jugendlichen zu einer reflektierten und mündigen Mediennutzung befähigt. Alle Inhalte sind auf die Zielgruppe abgestimmt und werden stetig mit Feedbackmethoden evaluiert, um den Projektverlauf an die Bedürfnisse der Lernenden anzupassen.

II. Beschreibung des Projektverlaufs

a) Konnten alle Projektinhalte umgesetzt werden?

Die Umsetzung aller geplanten Inhalte gelang weitestgehend, obwohl der Zeitrahmen bei einigen Teilbereichen, insbesondere bei der Produktion von Podcasts und Kurzvideos, enger als erwartet wurde. Die Jugendlichen haben jedoch alle Bausteine durchlaufen können und sowohl **theoretisches** als auch **praktisches** Wissen erworben. Zu Beginn standen Einheiten zu Big Data, Datenschutz und DSGVO auf dem Lehrplan, gefolgt von konkreten Übungen zu Recherche, Themenauswahl und Planung. Anschließend entstanden unterschiedliche Medienprodukte, in denen die Lernenden ihre erworbenen Kenntnisse kreativ umsetzten.

Bei der Umsetzung half zudem die begleitende Reflexion: In regelmäßigen Abständen wurden Zwischenergebnisse diskutiert, Feedback eingeholt und Anpassungen vorgenommen. Technische oder organisatorische Schwierigkeiten konnten zumindest teilweise aufgefangen werden. Der Einsatz von KI-Tools (z. B. ChatGPT) verlief ebenfalls erfolgreich, jedoch war hier eine intensivere Betreuung nötig, um die Lernenden an ethische und qualitative Aspekte heranzuführen und so einen kritischen Umgang zu ermöglichen. Insbesondere in der Content-Erstellung wurde seitens der Schülerinnen und Schüler auf KI-Tools zurückgegriffen.

b) Wie wurden die Kinder/Jugendlichen eingebunden?

Von Anfang an wurde ein partizipativer Ansatz verfolgt: Die Jugendlichen bildeten **Arbeitsgruppen**, in denen sie eigenverantwortlich Themen auswählten, Rollen verteilten und Aufgaben koordinierten. Dieser Ansatz förderte ihre Eigeninitiative und das Bewusstsein, dass sie selbst Gestaltende in einem größeren Projekt sind. Die Lehrkraft agierte eher als **Coach** und gab methodische Hilfestellungen oder vermittelte Fachwissen zu Big Data und Datenschutz, während die tatsächliche Umsetzung weitgehend in den Händen der Jugendlichen lag.

Darüber hinaus kamen **digitale Feedback-Tools** zum Einsatz, zum Beispiel „Edkimo“, um auf Grundlage konkreter Rückmeldungen fortlaufend Anpassungen in der Projektstruktur oder Aufgabenverteilung vorzunehmen. Positionierungsspiele und kurze Reflexionsrunden unterstützten zusätzlich die Einbindung aller Teilnehmenden, sodass auch leisere Stimmen Gehör fanden. Auf diese Weise waren die Jugendlichen inhaltlich und methodisch bestmöglich involviert, sodass eine hohe Identifikation mit den erarbeiteten Themen entstand.

c) Welche Aufgaben wurden von den Kindern/Jugendlichen wahrgenommen?

Die Aufgabengebiete waren vielfältig und eröffneten den Teilnehmenden die Möglichkeit, ihre individuellen Fähigkeiten einzubringen:

- **Podcast-Produktion:** Recherche zu Big Data und DSGVO, Erstellen und Formulieren von Interviewleitfäden, technische Durchführung von Aufnahmen, Audibearbeitung und Schnitt.
- **Kurzvideo-Erstellung:** Entwicklung von Drehbüchern, Erlernen von Kameratechniken, Beleuchtungssetup, Schnitt und Postproduktion mit entsprechender Software.
- **Infolyer-Gestaltung:** Reduktion komplexer Inhalte, Layout-Gestaltung, Einbau rechtlicher Hinweise (DSGVO) und ansprechende Visualisierung.
- **Social-Media-Kampagnen:** Konzeption einer themenspezifischen Kampagne, Posting-Strategien, Hashtag-Recherche, Reichweiten-Analyse und Community-Interaktion.
- **Einsatz von KI-Tools:** Nutzung von ChatGPT zur Content-Erstellung, begleitende Analyse von KI-generierten Inhalten auf Richtigkeit und ethische Implikationen.
- **Politische Medienbildung:** Recherche zu manipulativem Social-Media-Content und Diskussion darüber, wie politische Prozesse – etwa bei Wahlen in den USA oder Rumänien – gezielt beeinflusst werden können.

Diese Bandbreite an Aufgaben ließ die Jugendlichen eigenverantwortlich arbeiten und förderte sowohl ihre kreativen als auch organisatorischen Fähigkeiten. Dabei gewannen sie einen Einblick in die vielseitigen Prozesse der Medienproduktion und entwickelten ein stärkeres Bewusstsein für Datenschutz und Manipulationsgefahren.

III. Bewertung des Projektverlaufs

a) Was lief besonders positiv oder negativ während der Projektdurchführung?

Besonders positiv hervorzuheben ist die hohe **Motivation** der Jugendlichen, sobald sie in der Lage waren, **eigene** Medienprodukte zu erstellen. Das selbstbestimmte Arbeiten weckte eine kreative Dynamik: In den Gruppen herrschte reger Ideenaustausch, es wurde experimentiert und ausprobiert. Die Ergebnisse – seien es Podcast-Episoden, Kurzvideos oder Infoflyer – sind qualitativ überzeugend, was sich auch in den Rückmeldungen der Teilnehmenden widerspiegelt. Sie schätzten insbesondere die praxisnahe Herangehensweise, die ihnen half, komplexe Themen wie Big Data oder die DSGVO greifbar zu machen.

Negativ zu bewerten ist jedoch, dass der **Zeitfaktor** eine Herausforderung darstellte, da sowohl die Einarbeitung in die nötige Software als auch das Erlernen von Aufnahme- und Schnitttechniken mehr Zeit in Anspruch nahm als ursprünglich veranschlagt. Ein weiterer Punkt war die teils **intensive Betreuung** beim Einsatz von KI-Tools, weil einige Schülerinnen und Schüler Schwierigkeiten hatten, die generierten Inhalte fundiert zu bewerten. Insgesamt minderten diese Aspekte aber nicht das generelle Engagement und den Lernerfolg, sondern zeigten lediglich, wo Verbesserungspotenzial liegt.

b) Was würden Sie verbessern wollen?

Professionellere Mikrofone, Kameras oder auch der Zugang zu leistungsfähiger Software könnte die Qualität der Arbeitsergebnisse weiter steigern. Gleichzeitig sollten **Workshops zur ethischen KI-Nutzung** intensiviert werden, damit die Jugendlichen noch gezielter lernen, KI-generierte Inhalte kritisch zu hinterfragen.

Ein weiterer Punkt betrifft das **Zeitmanagement**: Eine detailliertere Zeitplanung mit Pufferphasen für technische Probleme oder Schulungen im Umgang mit neuen Tools könnte den Druck von den Lernenden nehmen und den Fokus verstärkt auf eine vertiefte inhaltliche Auseinandersetzung legen. Zudem ist denkbar, über **externe Kooperationspartner** (z. B. Medienhäuser oder Vereine) zusätzliche Unterstützung in Form von Praxis-Workshops einzuholen, wenngleich dies bislang noch nicht umgesetzt wurde.

c) Werden Sie zukünftig medienpädagogische Projekte in Ihrer Einrichtung durchführen?

Die durchweg positiven Erfahrungen und die hohe Akzeptanz des Projekts bei den Lernenden haben gezeigt, dass **medienpädagogische Projekte** einen enormen Mehrwert für den Schulalltag bieten. Insbesondere der direkte Praxisbezug, die Verknüpfung mit lebensweltlichen Themen (etwa Datenschutz in sozialen Netzwerken) sowie die Entwicklung politischer Mündigkeit sprechen dafür, solche Projekte weiter auszubauen. Da „Big Data vs. DSGVO“ Teil des übergeordneten Konzepts **„Medienkompetenz messbar machen“** ist, ist bereits eine längerfristige Integration und Weiterentwicklung in der schulischen Praxis geplant.

d) Welche Erfahrungen nehmen Sie mit?

Das Projekt hat verdeutlicht, dass eine Kombination aus **theoretischer Grundlage** und **praktischer Umsetzung** die effektivste Methode ist, Jugendlichen komplexe Inhalte zu vermitteln. So wurde beispielsweise Datenschutz durch die **eigene Medienproduktion** unmittelbar greifbar und verständlich. Gleichzeitig zeigt der Erfolg, dass ein **kritischer Umgang mit KI-Tools** erlernt werden kann, wenn entsprechende Betreuung und Reflexionsangebote vorhanden sind.

Darüber hinaus wurde klar, welche Bedeutung die Sensibilisierung für **Desinformation** und **manipulative Medieninhalte** hat. Insbesondere die Beispiele zu Wahlkämpfen in den USA oder Rumänien und die damit verbundene Nutzung sozialer Netzwerke haben ein Bewusstsein dafür geschaffen, dass sich politische Prozesse und das eigene Handeln im Netz gegenseitig beeinflussen. So entstand eine **Stärkung der demokratischen Handlungskompetenz**, indem Jugendliche lernten, Quellen kritisch zu prüfen und aktiv gegen potenzielle Falschmeldungen Position zu beziehen.

Insgesamt bleibt festzuhalten, dass „Big Data vs. DSGVO“ als zeitgemäßes Medienprojekt den Nerv der Jugendlichen getroffen hat. Die positiven Rückmeldungen zeigen, dass solche Projekte die **Medienmündigkeit** nachhaltig fördern und gleichzeitig wichtige Zukunftskompetenzen vermitteln. Durch die Anbindung an „Medienkompetenz messbar machen“ ist zudem gewährleistet, dass diese Form der medienpädagogischen Arbeit langfristig in das Schulcurriculum eingebettet wird.

Dieses Projekt wurde unter gezieltem Einsatz von KI-gestützten Werkzeugen entwickelt. Die initiale Projektbeschreibung entstand in Zusammenarbeit mit ChatGPT und wurde anschließend durch den Projekteinreichenden individuell angepasst und verfeinert. Auch die Schülerergebnisse profitierten von der kreativen Unterstützung durch Sprachmodelle wie ChatGPT oder Google Gemini, wobei die Inhalte durch die Schüler weitergedacht und eigenständig entwickelt wurden.

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

SCHATTENPROFILE

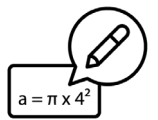
Shadow Profiles sind u.a. versteckte Online-Profile von Menschen, die durch das Sammeln von Daten entstanden sind, ohne dass diese Menschen die Profile selbst angelegt haben. Sie entstehen durch Cookies, geteilte Adressbücher, geteilte Accounts uvm. In der Vergangenheit sind sie vor allem durch die "Facebook Pixel" bekannt geworden und spielen politisch, gesellschaftlich und juristisch eine entscheidende Rolle in der Onlinewelt.

PODCAST

Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



Was sind Schattenprofile?

Schattenprofile, auch "Shadow Profiles" genannt, entstehen durch das Sammeln von Daten über Personen, die selbst keine Nutzer der entsprechenden Plattform sind. Facebook, eines der bekanntesten Beispiele, sammelt Informationen durch verschiedene Methoden wie das Hochladen von Adressbüchern, Cookies oder durch die Verbindungen von Freunden und Kontakten der Nutzer. So kann das Unternehmen detaillierte Profile von Menschen erstellen, die selbst nie einen Account bei Facebook hatten.

Diese Daten können über verschiedene Quellen zusammengetragen werden, z. B. durch "Facebook Pixel" auf Websites oder durch andere Dienste, die Daten an Facebook/Meta-Konzern weiterleiten. Ein Problem bei dieser Praxis ist, dass Betroffene oft keine Kontrolle darüber haben, welche Informationen gesammelt werden. Sie haben auch keine Möglichkeit, diese Profile einzusehen oder zu löschen, da sie nicht direkt mit einem Account verknüpft sind.

Darüber hinaus geht die Sammlung oft über grundlegende Kontaktinformationen hinaus. Es werden Interessen, soziale Netzwerke und Online-Verhalten analysiert, um gezielte Werbung zu schalten und das Verhalten vorherzusagen. Dies führt zu umfassenden Datensätzen, die eine Gefahr für die Privatsphäre darstellen können, da sie ohne Einwilligung der betroffenen Personen erstellt werden.

Die Datenschutz-Grundverordnung (DSGVO) der EU fordert eigentlich ein hohes Maß an Schutz für personenbezogene Daten, aber Unternehmen wie Facebook argumentieren oft mit einem "berechtigten Interesse" an diesen Informationen, um diese Praxis fortzuführen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die in Schattenprofilen gespeichert werden?
- Welche Regeln der DSGVO schützen Nutzer:innen davor, dass Schattenprofile erstellt werden? Gehe dabei auf das Recht auf informierte Einwilligung ein.
- Wie beeinflussen Schattenprofile die Privatsphäre der Nutzer:innen? Welche Privatsphäre-Risiken gibt es, wenn beispielsweise der Konzern Meta (Facebook, Instagram, Threads, WhatsApp) Informationen der verschiedenen Plattformen miteinander verknüpft?
- Was passiert mit urheberrechtlich geschützten Daten (Bilder, Videos, ...)? Was ist das „Recht am eigenen Bild“?
- Wie kann man sein Schattenprofil löschen lassen? Recherchiere das „Recht auf Vergessenwerden“.

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



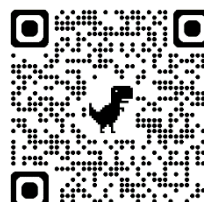
QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



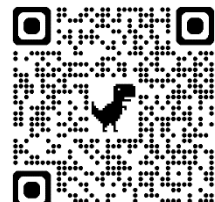
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am
eigenen Bild

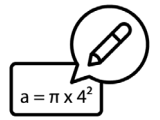


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- Netzpolitik.org:
<https://netzpolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an/>
- Taz.de:
<https://taz.de/Schattenprofile-im-Netz/!5967472/>
- Scinexx.de:
<https://www.scinexx.de/dossier/die-daten-der-anderen-shadow-profiles/>
- Juuuport.de:
<https://www.juuuport.de/infos/news/wie-du-fake-profile-erkennen-kannst>
- Campus.uni-konstanz.de:
<https://www.campus.uni-konstanz.de/wissenschaft/die-daten-der-anderen-shadow-profiles>

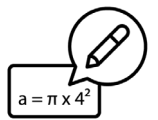


Podcast-Fragen: Schattenprofile & Meta

1. **Was ist ein Schattenprofil und wie wird es erstellt?**
 - (Ziel: Erklärung des Begriffs und der Mechanismen hinter der Erstellung von Schattenprofilen)
2. **Wie sammelt Meta (Facebook, WhatsApp, Instagram, Threads) Daten über Nutzer, auch wenn diese nicht aktiv zugestimmt haben?**
 - (Ziel: Untersuchung der Datenerhebungsmethoden bei Meta, selbst für Nicht-Nutzer oder inaktiven Nutzer)
3. **Welche Rolle spielt die DSGVO beim Schutz vor der Erstellung von Schattenprofilen?**
 - (Ziel: Erklärung, wie die DSGVO versucht, Nutzerdaten zu schützen und die Einwilligungspflicht sicherzustellen)
4. **Inwieweit können Nutzer bei Meta-Plattformen kontrollieren, welche Daten über sie gesammelt werden, und wie transparent ist der Konzern dabei?**
 - (Ziel: Diskussion über die Privatsphäre-Einstellungen und die Transparenz der Datennutzung durch Meta)
5. **Gibt es rechtliche Möglichkeiten für Nutzer, die Löschung von Schattenprofilen zu verlangen (Stichwort: Recht auf Vergessenwerden)?**
 - (Ziel: Untersuchung der rechtlichen Rechte der Nutzer in Bezug auf ihre Daten und die Möglichkeit, Profile löschen zu lassen)
6. **Wie geht Meta mit dem Recht am eigenen Bild um? Können Bilder, die auf Instagram oder Facebook geteilt werden, Teil eines Schattenprofils werden?**
 - (Ziel: Verbindung zwischen Bildrechten und der Verwendung von Bildern in Schattenprofilen)
7. **Welche aktuellen Problematiken siehst du in der Kombination von Schattenprofilen und personalisierter Werbung auf Meta-Plattformen?**
 - (Ziel: Thematisierung der ethischen und rechtlichen Fragestellungen rund um die Nutzung von Schattenprofilen für Werbezwecke)
8. **Was sollten Nutzer tun, wenn sie vermuten, dass ein Schattenprofil von ihnen existiert? Welche Rechte haben sie?**
 - (Ziel: Praktische Ratschläge für Nutzer, wie sie ihre Rechte wahrnehmen können)
9. **Wie unterscheidet sich die Datenerfassung bei den verschiedenen Plattformen von Meta (z.B. WhatsApp vs. Instagram)?**
 - (Ziel: Aufzeigen der Unterschiede bei der Datenerhebung auf den verschiedenen Meta-Diensten)
10. **Inwiefern betrifft das Problem der Schattenprofile auch Personen, die gar keinen Account bei Meta haben?**
 - (Ziel: Erklärung, dass Daten auch von Nicht-Nutzern durch Interaktionen mit Meta-Nutzern gesammelt werden können)



SCHATTENPROFILE



Was sind Schattenprofile?

Schattenprofile, auch "Shadow Profiles" genannt, entstehen durch das Sammeln von Daten über Personen, die selbst keine Nutzer der entsprechenden Plattform sind. Facebook, eines der bekanntesten Beispiele, sammelt Informationen durch verschiedene Methoden wie das Hochladen von Adressbüchern, Cookies oder durch die Verbindungen von Freunden und Kontakten der Nutzer. So kann das Unternehmen detaillierte Profile von Menschen erstellen, die selbst nie einen Account bei Facebook hatten.

Diese Daten können über verschiedene Quellen zusammengetragen werden, z. B. durch "Facebook Pixel" auf Websites oder durch andere Dienste, die Daten an Facebook/Meta-Konzern weiterleiten. Ein Problem bei dieser Praxis ist, dass Betroffene oft keine Kontrolle darüber haben, welche Informationen gesammelt werden. Sie haben auch keine Möglichkeit, diese Profile einzusehen oder zu löschen, da sie nicht direkt mit einem Account verknüpft sind.

Darüber hinaus geht die Sammlung oft über grundlegende Kontaktinformationen hinaus. Es werden Interessen, soziale Netzwerke und Online-Verhalten analysiert, um gezielte Werbung zu schalten und das Verhalten vorherzusagen. Dies führt zu umfassenden Datensätzen, die eine Gefahr für die Privatsphäre darstellen können, da sie ohne Einwilligung der betroffenen Personen erstellt werden.

Die Datenschutz-Grundverordnung (DSGVO) der EU fordert eigentlich ein hohes Maß an Schutz für personenbezogene Daten, aber Unternehmen wie Facebook argumentieren oft mit einem "berechtigten Interesse" an diesen Informationen, um diese Praxis fortzuführen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die in Schattenprofilen gespeichert werden?
- Welche Regeln der DSGVO schützen Nutzer:innen davor, dass Schattenprofile erstellt werden? Gehe dabei auf das Recht auf informierte Einwilligung ein.
- Wie beeinflussen Schattenprofile die Privatsphäre der Nutzer:innen? Welche Privatsphäre-Risiken gibt es, wenn beispielsweise der Konzern Meta (Facebook, Instagram, Threads, WhatsApp) Informationen der verschiedenen Plattformen miteinander verknüpft?
- Was passiert mit urheberrechtlich geschützten Daten (Bilder, Videos, ...)? Was ist das „Recht am eigenen Bild“?
- Wie kann man sein Schattenprofil löschen lassen? Recherchiere das „Recht auf Vergessenwerden“.

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze iMovie/Clips zum Erstellen und Bearbeiten der Inhalte.



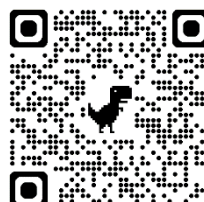
QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



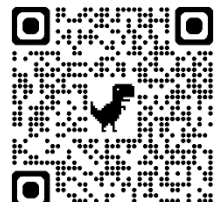
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am
eigenen Bild

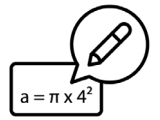


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- Netropolitik.org:
<https://netropolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an/>
- Taz.de:
<https://taz.de/Schattenprofile-im-Netz/!5967472/>
- Scinexx.de:
<https://www.scinexx.de/dossier/die-daten-der-anderen-shadow-profiles/>
- Juuuport.de:
<https://www.juuuport.de/infos/news/wie-du-fake-profile-erkennen-kannst>
- Campus.uni-konstanz.de:
<https://www.campus.uni-konstanz.de/wissenschaft/die-daten-der-anderen-shadow-profiles>



Szene: „Dein Schattenprofil und der Algorithmus“

Ort: Ein Café, zwei Personen sitzen an einem Tisch und trinken Kaffee. Person A scrollt durch Instagram auf ihrem Smartphone. Person B beobachtet das und startet das Gespräch.

Person A (auf das Smartphone schauend):

„Hey, ich bekomme hier die ganze Zeit Werbung für Klamotten, die ich mir nie angeschaut habe. Voll creepy.“

Person B (lächelnd):

„Das liegt wahrscheinlich an deinem Schattenprofil und dem Algorithmus.“

Person A (verwundert):

„Schattenprofil? Algorithmus? Was meinst du?“

Person B (lehnt sich vor):

„Also, ein Schattenprofil ist ein verstecktes Profil, das Plattformen wie Facebook, Instagram und WhatsApp über dich anlegen, basierend auf deinen Aktivitäten. Und der Algorithmus nutzt all diese Daten, um dir personalisierte Inhalte und Werbung zu zeigen.“

Person A (schockiert):

„Moment mal, die wissen alles über mich, obwohl ich nichts bewusst geteilt habe? Wie funktioniert das?“

Person B (ernst):

„Der Algorithmus analysiert alles – was du likest, anschaust, und sogar, mit wem du auf WhatsApp schreibst. Auch wenn du keine persönlichen Infos direkt eingibst, kann er anhand deines Verhaltens ein Profil von dir erstellen.“

Person A (erschrocken):

„Aber das kann doch nicht erlaubt sein!“

Person B (nickt):

„Eigentlich schützt uns die DSGVO davor. Du hast das Recht zu erfahren, welche Daten gesammelt werden, und du kannst sogar verlangen, dass sie gelöscht werden – das nennt man das 'Recht auf Vergessenwerden'. Aber der Algorithmus arbeitet ständig weiter.“

Person A (zweifelnd):

„Und wie mache ich das?“

Person B (ruhig):

„Meta und andere Plattformen verstecken die Optionen gut, aber du kannst verlangen, dass dein Schattenprofil gelöscht wird. Es ist ein bisschen aufwendig, aber es lohnt sich, den Algorithmus in Schach zu halten und deine Privatsphäre zu schützen.“

Person A (entschlossen):

„Das klingt, als müsste ich mich mal wirklich darum kümmern.“

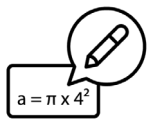
Schlusszene:

Text auf dem Bildschirm:

„Wissen ist Macht. Schütze deine Daten vor dem Algorithmus. #RechtaufVergessenwerden #DSGVO #Schattenprofil“

Voiceover:

„Erfahre, was der Algorithmus über dich weiß. Fordere deine Daten ein und schütze deine Privatsphäre.“



Was sind Schattenprofile?

Schattenprofile, auch "Shadow Profiles" genannt, entstehen durch das Sammeln von Daten über Personen, die selbst keine Nutzer der entsprechenden Plattform sind. Facebook, eines der bekanntesten Beispiele, sammelt Informationen durch verschiedene Methoden wie das Hochladen von Adressbüchern, Cookies oder durch die Verbindungen von Freunden und Kontakten der Nutzer. So kann das Unternehmen detaillierte Profile von Menschen erstellen, die selbst nie einen Account bei Facebook hatten.

Diese Daten können über verschiedene Quellen zusammengetragen werden, z. B. durch "Facebook Pixel" auf Websites oder durch andere Dienste, die Daten an Facebook/Meta-Konzern weiterleiten. Ein Problem bei dieser Praxis ist, dass Betroffene oft keine Kontrolle darüber haben, welche Informationen gesammelt werden. Sie haben auch keine Möglichkeit, diese Profile einzusehen oder zu löschen, da sie nicht direkt mit einem Account verknüpft sind.

Darüber hinaus geht die Sammlung oft über grundlegende Kontaktinformationen hinaus. Es werden Interessen, soziale Netzwerke und Online-Verhalten analysiert, um gezielte Werbung zu schalten und das Verhalten vorherzusagen. Dies führt zu umfassenden Datensätzen, die eine Gefahr für die Privatsphäre darstellen können, da sie ohne Einwilligung der betroffenen Personen erstellt werden.

Die Datenschutz-Grundverordnung (DSGVO) der EU fordert eigentlich ein hohes Maß an Schutz für personenbezogene Daten, aber Unternehmen wie Facebook argumentieren oft mit einem "berechtigten Interesse" an diesen Informationen, um diese Praxis fortzuführen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die in Schattenprofilen gespeichert werden?
- Welche Regeln der DSGVO schützen Nutzer:innen davor, dass Schattenprofile erstellt werden? Gehe dabei auf das Recht auf informierte Einwilligung ein.
- Wie beeinflussen Schattenprofile die Privatsphäre der Nutzer:innen? Welche Privatsphäre-Risiken gibt es, wenn beispielsweise der Konzern Meta (Facebook, Instagram, Threads, WhatsApp) Informationen der verschiedenen Plattformen miteinander verknüpft?
- Was passiert mit urheberrechtlich geschützten Daten (Bilder, Videos, ...)? Was ist das „Recht am eigenen Bild“?
- Wie kann man sein Schattenprofil löschen lassen? Recherchiere das „Recht auf Vergessenwerden“.

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



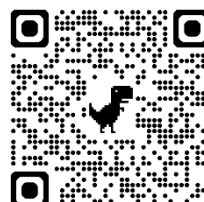
QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



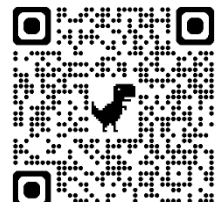
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am
eigenen Bild



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

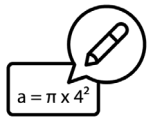


Weitere Quellen:

- Netropolitik.org:
<https://netropolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an/>
- Taz.de:
<https://taz.de/Schattenprofile-im-Netz/!5967472/>
- Scinexx.de:
<https://www.scinexx.de/dossier/die-daten-der-anderen-shadow-profiles/>
- Juuuport.de:
<https://www.juuuport.de/infos/news/wie-du-fake-profile-erkennen-kannst>
- Campus.uni-konstanz.de:
<https://www.campus.uni-konstanz.de/wissenschaft/die-daten-der-anderen-shadow-profiles>



SCHATTENPROFILE



Flyer-Design: „Schon gewusst?“ – Schattenprofile und Datenschutz (KI-generiert)

Layout:

1. **Größe des Flyers:** A5 (einseitig).
2. **Farbgestaltung:** Ein modernes, professionelles Design mit **Schattierungen von Blau und Weiß**. Blau vermittelt Vertrauen und Technologie, während Weiß den Flyer sauber und gut lesbar macht.



1. Überschrift:

- **Position:** Oben auf dem Flyer, zentriert.
- **Text:** „Schon gewusst?“ in **großer, fetter Schrift**.
- **Schriftart:** Eine moderne, klare Schriftart (z.B. Arial oder Helvetica).
- **Farbe:** Blau, um die Aufmerksamkeit zu erregen.

2. Einleitender Text:

- **Position:** Direkt unter der Überschrift.
- **Text:** Eine kurze Erklärung, die Schattenprofile und die Datensammlung durch Plattformen wie Meta beschreibt. Der Text sollte in **einem kurzen Absatz** zusammengefasst werden.
- **Schriftart:** Etwas kleiner als die Überschrift, aber gut lesbar.
- **Farbe:** Schwarz oder dunkles Grau für klare Lesbarkeit.

3. Fakten und Tipps:

- **Position:** In der Mitte des Flyers, als **Liste** angeordnet.
- **Text:** Eine Liste mit 3–4 Tipps zum Schutz der Daten, z.B. „Überprüfe deine Privatsphäre-Einstellungen“, „Nutze das Recht auf Vergessenwerden“.
- **Schriftart:** Leicht hervorgehoben (z.B. fett oder kursiv), damit die Tipps gut ins Auge fallen.
- **Farbe:** Schwarz für den Text, eventuell mit **Blau** für Aufzählungspunkte oder Nummern, um die Liste hervorzuheben.

4. Grafik/Symbol:

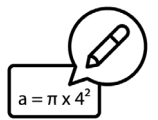
- **Position:** Unten rechts auf dem Flyer.
- **Bild:** Ein einfaches **Schloss** oder **Schild**, das für Datenschutz und Sicherheit steht.
- **Größe:** Klein und dezent, damit es den Text nicht überlagert, aber das Thema visuell unterstreicht.

5. Abschlusssatz:

- **Position:** Unten links oder zentriert, neben der Grafik.
- **Text:** „Bleib informiert und schütze deine Daten. #DSGVO #Schattenprofil #Privatsphäre“.
- **Schriftart:** Klein und fein, aber gut lesbar.
- **Farbe:** Blau oder Grau, um harmonisch zum Rest des Designs zu passen.

Gestaltungstipps:

- Nutzt **weißen Raum**, um den Flyer nicht zu überladen. Jeder Abschnitt sollte gut voneinander getrennt sein.
- **Symmetrie** hilft, das Design ordentlich und professionell wirken zu lassen.
- **Icons** oder kleine Grafiken können an den Rändern oder in der Mitte der Seite eingefügt werden, um den Flyer ansprechender zu gestalten.



Was sind Schattenprofile?

Schattenprofile, auch "Shadow Profiles" genannt, entstehen durch das Sammeln von Daten über Personen, die selbst keine Nutzer der entsprechenden Plattform sind. Facebook, eines der bekanntesten Beispiele, sammelt Informationen durch verschiedene Methoden wie das Hochladen von Adressbüchern, Cookies oder durch die Verbindungen von Freunden und Kontakten der Nutzer. So kann das Unternehmen detaillierte Profile von Menschen erstellen, die selbst nie einen Account bei Facebook hatten.

Diese Daten können über verschiedene Quellen zusammengetragen werden, z. B. durch "Facebook Pixel" auf Websites oder durch andere Dienste, die Daten an Facebook/Meta-Konzern weiterleiten. Ein Problem bei dieser Praxis ist, dass Betroffene oft keine Kontrolle darüber haben, welche Informationen gesammelt werden. Sie haben auch keine Möglichkeit, diese Profile einzusehen oder zu löschen, da sie nicht direkt mit einem Account verknüpft sind.

Darüber hinaus geht die Sammlung oft über grundlegende Kontaktinformationen hinaus. Es werden Interessen, soziale Netzwerke und Online-Verhalten analysiert, um gezielte Werbung zu schalten und das Verhalten vorherzusagen. Dies führt zu umfassenden Datensätzen, die eine Gefahr für die Privatsphäre darstellen können, da sie ohne Einwilligung der betroffenen Personen erstellt werden.

Die Datenschutz-Grundverordnung (DSGVO) der EU fordert eigentlich ein hohes Maß an Schutz für personenbezogene Daten, aber Unternehmen wie Facebook argumentieren oft mit einem "berechtigten Interesse" an diesen Informationen, um diese Praxis fortzuführen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die in Schattenprofilen gespeichert werden?
- Welche Regeln der DSGVO schützen Nutzer:innen davor, dass Schattenprofile erstellt werden? Gehe dabei auf das Recht auf informierte Einwilligung ein.
- Wie beeinflussen Schattenprofile die Privatsphäre der Nutzer:innen? Welche Privatsphäre-Risiken gibt es, wenn beispielsweise der Konzern Meta (Facebook, Instagram, Threads, WhatsApp) Informationen der verschiedenen Plattformen miteinander verknüpft?
- Was passiert mit urheberrechtlich geschützten Daten (Bilder, Videos, ...)? Was ist das „Recht am eigenen Bild“?
- Wie kann man sein Schattenprofil löschen lassen? Recherchiere das „Recht auf Vergessenwerden“.

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



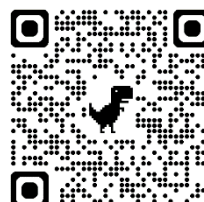
QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



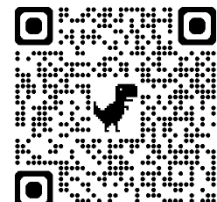
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am
eigenen Bild



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

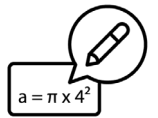


Weitere Quellen:

- Netzpolitik.org:
<https://netzpolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an/>
- Taz.de:
<https://taz.de/Schattenprofile-im-Netz/!5967472/>
- Scinexx.de:
<https://www.scinexx.de/dossier/die-daten-der-anderen-shadow-profiles/>
- Juuuport.de:
<https://www.juuuport.de/infos/news/wie-du-fake-profile-erkennen-kannst>
- Campus.uni-konstanz.de:
<https://www.campus.uni-konstanz.de/wissenschaft/die-daten-der-anderen-shadow-profiles>



SCHATTENPROFILE



1. Kampagnenziel: Das Ziel der Kampagne ist es, Schüler, Eltern und die Schulgemeinde über Schattenprofile, Algorithmen und den Schutz ihrer persönlichen Daten aufzuklären.

2. Beiträge der Kampagne:

Beitrag 1: Podcast-Ankündigung

- Bild/Video: Ein einfaches, animiertes Bild mit dem Titel „Was sind Schattenprofile?“ und einem Play-Button-Icon.
- Text (Post-Beschreibung): „🔊 Schon gewusst? Meta (Facebook, Instagram, WhatsApp) sammelt viele Daten über dich, auch wenn du sie nicht aktiv preisgibst. In unserem neuen Podcast sprechen wir darüber, was Schattenprofile sind, wie sie entstehen und was du dagegen tun kannst! ➡ Hör jetzt rein und schütze deine Daten! #Schattenprofile #Datenschutz #DSGVO #Meta“
- Link im Bio: Zum Podcast (z.B. auf SoundCloud oder einem Schulserver).
- Story: Ein kurzes Teaser-Video mit der Frage: „Weißt du, was ein Schattenprofil ist? Klick auf den Link in unserer Bio, um mehr zu erfahren!“ mit einem Swipe-up-Link zum Podcast.

Beitrag 2: 2-Minuten-Video „Dein Schattenprofil“

- Bild/Video: Das 2-minütige Erklärvideo, das eine Unterhaltung zwischen zwei Personen zeigt, die über Schattenprofile und den Algorithmus sprechen.
- Text (Post-Beschreibung): „👁️ Was weiß Meta über dich? In nur 2 Minuten erfährst du, wie Schattenprofile entstehen und wie der Algorithmus dich beeinflusst. Schau dir unser neues Video an! #Schattenprofile #Algorithmen #Datensicherheit #SchutzdeinerDaten“
- Story: Ein kurzer Clip des Videos mit einem Call-to-Action: „Wusstest du, dass jede deiner Aktionen auf Social Media aufgezeichnet wird? Schau dir unser Video an, um zu erfahren, wie du deine Privatsphäre schützen kannst!“

Beitrag 3: Aufklärungsflyer

- Bild: Der digitale Flyer über Schattenprofile und Datenschutz.
- Text (Post-Beschreibung): „📄 Lade unseren kostenlosen Flyer herunter und erfahre, wie du deine Daten schützen kannst! Schau dir unsere Tipps an, wie du Schattenprofile vermeidest und dein Recht auf Vergessenwerden nutzt. Link in Bio! #Flyer #Datenschutz #DSGVO #Schattenprofile #SicherimNetz“
- Story: Ein Swipe-up-Link zum Download des Flyers (z.B. über Google Drive oder Schul-Website) mit der Nachricht: „Hol dir unseren Flyer und informiere dich über deine Rechte im Netz!“

3. Zusätzliche Posts/Stories zur Erhöhung der Reichweite:

Post-Idee 1: Quiz zur Privatsphäre

- Bild: Ein interaktives Bild, das eine Quiz-Frage stellt (z.B. „Weißt du, wie viele Daten Facebook über dich sammelt?“) mit einer Auswahl an Antworten.
- Text: „Teste dein Wissen über Datenschutz! Wie gut kennst du die Daten, die täglich über dich gesammelt werden? Nimm an unserem Quiz teil und finde es heraus!“

Post-Idee 2: Fakten über Schattenprofile

- Bild: Eine Infografik mit Fakten über Schattenprofile (z.B. „Jede Bewegung hinterlässt eine Spur im Netz“).
- Text: „Schon gewusst? Auch wenn du nichts postest, hinterlässt du Spuren. Schattenprofile entstehen, wenn Plattformen wie Meta deine Daten nutzen. Erfahre, wie du dich schützen kannst! #Datenschutz #Algorithmen #Privatsphäre“

Story-Idee: Umfrage zur Nutzung von Social Media

- Frage: „Weißt du, wie du deine Privatsphäre-Einstellungen anpasst?“
- Optionen: „Ja, total wichtig!“ / „Nein, wie geht das?“
- Ergebnis: Bei „Nein“ könnten sie zu einem Tutorial-Post weitergeleitet werden.

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

KRANKENKASSEN UND WEARABLES

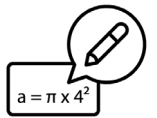
Wearables wie SmartWatches, smarte Ringe oder Fitnesstracker dienen dazu Gesundheitsdaten zu sammeln und auszuwerten. Sie sammeln kontinuierlich die privatesten Daten eines Menschen: Herzfrequenz, Sauerstoffsättigung, Bewegung, uvm. und erstellen ein persönliches Profil daraus. Für Autoversicherungen gibt es bereits den Telematik-Tarif. Wird das auch für Krankenversicherungen kommen?

PODCAST

Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



Was haben Krankenkassen mit meiner Smartwatch zu tun?

Krankenkassen und Wearables bieten ein anschauliches Beispiel für den Einsatz von Big Data im Gesundheitswesen. Wearables wie Fitness-Tracker, Smartwatches und andere vernetzte Geräte erfassen kontinuierlich Gesundheitsdaten wie Herzfrequenz, Schlafmuster, Bewegungsaktivität oder Kalorienverbrauch. Diese Daten können in Kombination mit Gesundheits-Apps und digitalen Plattformen gesammelt und ausgewertet werden.

Immer mehr Krankenkassen bieten Anreize an, um Versicherte dazu zu bewegen, ihre Wearable-Daten zu teilen. Ein Beispiel hierfür sind Bonusprogramme: Versicherte erhalten Prämien oder Vergünstigungen, wenn sie nachweisen, dass sie bestimmte Gesundheitsziele erreichen, wie z. B. eine bestimmte Anzahl von Schritten pro Tag oder das Einhalten eines Trainingsplans. Durch das Teilen dieser Daten sollen Versicherte zu einem gesünderen Lebensstil motiviert werden, was in der Theorie langfristig auch die Krankheitskosten senken könnte.

Allerdings gibt es bei dieser Praxis auch erhebliche Bedenken in Bezug auf den Datenschutz und die Privatsphäre. Die gesammelten Daten über Wearables sind sehr persönlich und können tiefgreifende Einblicke in den Gesundheitszustand, den Lebensstil und sogar potenzielle Risiken geben. Eine große Frage ist, ob Versicherte durch den „freiwilligen“ Datenaustausch Nachteile erleiden könnten. Wenn jemand nicht bereit ist, seine Gesundheitsdaten zu teilen, könnte das als Indiz dafür gewertet werden, dass diese Person etwas zu verbergen hat oder potenziell ein höheres Gesundheitsrisiko darstellt. Dies könnte langfristig zu Ungleichheiten in den Beitragszahlungen führen.

Die Datenschutz-Grundverordnung (DSGVO) der EU spielt auch hier eine zentrale Rolle. Versicherte müssen klar und transparent darüber informiert werden, welche Daten gesammelt werden, wie sie verwendet werden und wie lange sie gespeichert bleiben. Sie müssen auch ihre ausdrückliche Einwilligung zur Datennutzung geben. Allerdings stellt sich die Frage, ob diese Einwilligung tatsächlich freiwillig ist, wenn Versicherte spürbare Vorteile erhalten, wenn sie zustimmen – oder potenziell Nachteile haben, wenn sie ablehnen.

Ein weiterer Aspekt ist, dass die Wearable-Daten oft in Echtzeit gesammelt und ausgewertet werden, was den Versicherern ermöglicht, sofortige Rückschlüsse auf das Verhalten der Versicherten zu ziehen. Diese dynamischen Daten können dazu führen, dass Krankenkassen nicht nur rückblickend auf das Gesundheitsverhalten blicken, sondern auch zukünftige Risiken vorhersagen und darauf basierend Prämien oder Behandlungsstrategien anpassen.



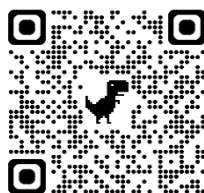
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die durch Wearables erhoben und bei der Krankenkasse gespeichert werden?
- Was passiert mit den Daten, die du durch Wearables wie Smartwatches und Fitness-Tracker teilst? Inwiefern sind diese Daten rechtlich geschützt?
- Welche Regeln der DSGVO/des Telemediengesetzes schützen dich davor, dass deine Wearable-Daten gegen dich verwendet werden?
- Wie kannst du sicherstellen, dass deine Wearable-Daten gelöscht werden? Recherchiere das „Recht auf Vergessenwerden“ in Bezug auf Krankenkassen und Gesundheitsdaten.

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



QR 1: DSGVO Art. 17
"Recht auf Vergessenwerden"



QR 2: DSGVO Art. 9
Verarbeitung personenbezogener Daten



QR 3:
Telemediengesetz



QR 4: DSGVO Art. 9,
Gesundheitsdaten

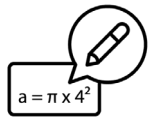


QR 5: DSGVO Art. 6
"Rechtmäßigkeit der Verarbeitung"



Weitere Quellen:

- Datenschutz-Notizen:
<https://www.datenschutz-notizen.de/die-vermessung-der-gesundheit-wie-positionieren-sich-krankenkassen-zu-wearables-1112189/>
- Datenschutzexperte.de:
<https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/datenschutz-im-gesundheitswesen/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/der-datenschutz-bei-krankenkassen/>



1. Podcast-Interviewer-Leitfaden (5-Minuten Podcast)

Thema:

Krankenkassen und Wearables: Chancen und Risiken durch Big Data

Interviewer-Leitfaden:

1. Einleitung:

- „Willkommen zu unserem Podcast. Heute sprechen wir über Krankenkassen und Wearables. Was passiert eigentlich mit den Daten, die dein Fitness-Tracker sammelt? Und wie nutzen Krankenkassen diese Daten?“

2. Frage 1:

„Wie sammeln Wearables wie Fitness-Tracker und Smartwatches Daten, und was für Daten sind das?“

- (Ziel: Grundlegende Einführung, wie Wearables Gesundheitsdaten, Fitnessdaten, Schlafrhythmen, Herzfrequenzen etc. aufzeichnen.)

3. Frage 2:

„Wie nutzen Krankenkassen diese Daten? Welche Vorteile haben Krankenkassen davon, Big Data aus Wearables zu analysieren?“

- (Ziel: Diskutieren, wie Krankenkassen diese Daten verwenden, um Präventionen anzubieten, Risiken einzuschätzen und Versicherungsbeiträge anzupassen.)

4. Frage 3:

„Was sagt die DSGVO über den Schutz von Gesundheitsdaten? Wie dürfen Krankenkassen und Wearable-Hersteller diese Daten nutzen?“

- (Ziel: Erklären der datenschutzrechtlichen Vorgaben der DSGVO, speziell den Umgang mit besonders schützenswerten Daten wie Gesundheitsdaten.)

5. Frage 4:

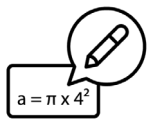
„Welche Risiken gibt es für die Privatsphäre der Nutzer, wenn ihre Daten von Krankenkassen analysiert werden?“

- (Ziel: Die potenziellen Gefahren und Missbrauchsmöglichkeiten durch Datenanalyse von Wearables besprechen.)

6. Frage 5:

„Wie können Nutzer ihre Daten schützen und ihr Recht auf Vergessenwerden wahrnehmen?“

- (Ziel: Praktische Tipps, wie Nutzer ihre Daten vor unkontrollierter Nutzung schützen können.)



Was haben Krankenkassen mit meiner Smartwatch zu tun?

Krankenkassen und Wearables bieten ein anschauliches Beispiel für den Einsatz von Big Data im Gesundheitswesen. Wearables wie Fitness-Tracker, Smartwatches und andere vernetzte Geräte erfassen kontinuierlich Gesundheitsdaten wie Herzfrequenz, Schlafmuster, Bewegungsaktivität oder Kalorienverbrauch. Diese Daten können in Kombination mit Gesundheits-Apps und digitalen Plattformen gesammelt und ausgewertet werden.

Immer mehr Krankenkassen bieten Anreize an, um Versicherte dazu zu bewegen, ihre Wearable-Daten zu teilen. Ein Beispiel hierfür sind Bonusprogramme: Versicherte erhalten Prämien oder Vergünstigungen, wenn sie nachweisen, dass sie bestimmte Gesundheitsziele erreichen, wie z. B. eine bestimmte Anzahl von Schritten pro Tag oder das Einhalten eines Trainingsplans. Durch das Teilen dieser Daten sollen Versicherte zu einem gesünderen Lebensstil motiviert werden, was in der Theorie langfristig auch die Krankheitskosten senken könnte.

Allerdings gibt es bei dieser Praxis auch erhebliche Bedenken in Bezug auf den Datenschutz und die Privatsphäre. Die gesammelten Daten über Wearables sind sehr persönlich und können tiefgreifende Einblicke in den Gesundheitszustand, den Lebensstil und sogar potenzielle Risiken geben. Eine große Frage ist, ob Versicherte durch den „freiwilligen“ Datenaustausch Nachteile erleiden könnten. Wenn jemand nicht bereit ist, seine Gesundheitsdaten zu teilen, könnte das als Indiz dafür gewertet werden, dass diese Person etwas zu verbergen hat oder potenziell ein höheres Gesundheitsrisiko darstellt. Dies könnte langfristig zu Ungleichheiten in den Beitragszahlungen führen.

Die Datenschutz-Grundverordnung (DSGVO) der EU spielt auch hier eine zentrale Rolle. Versicherte müssen klar und transparent darüber informiert werden, welche Daten gesammelt werden, wie sie verwendet werden und wie lange sie gespeichert bleiben. Sie müssen auch ihre ausdrückliche Einwilligung zur Datennutzung geben. Allerdings stellt sich die Frage, ob diese Einwilligung tatsächlich freiwillig ist, wenn Versicherte spürbare Vorteile erhalten, wenn sie zustimmen – oder potenziell Nachteile haben, wenn sie ablehnen.

Ein weiterer Aspekt ist, dass die Wearable-Daten oft in Echtzeit gesammelt und ausgewertet werden, was den Versicherern ermöglicht, sofortige Rückschlüsse auf das Verhalten der Versicherten zu ziehen. Diese dynamischen Daten können dazu führen, dass Krankenkassen nicht nur rückblickend auf das Gesundheitsverhalten blicken, sondern auch zukünftige Risiken vorhersagen und darauf basierend Prämien oder Behandlungsstrategien anpassen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die durch Wearables erhoben und bei der Krankenkasse gespeichert werden?
- Was passiert mit den Daten, die du durch Wearables wie Smartwatches und Fitness-Tracker teilst? Inwiefern sind diese Daten rechtlich geschützt?
- Welche Regeln der DSGVO/des Telemediengesetzes schützen dich davor, dass deine Wearable-Daten gegen dich verwendet werden?
- Wie kannst du sicherstellen, dass deine Wearable-Daten gelöscht werden? Recherchiere das „Recht auf Vergessenwerden“ in Bezug auf Krankenkassen und Gesundheitsdaten.

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, das alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze iMovie/Clips zum Erstellen und Bearbeiten der Inhalte.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Telemediengesetz



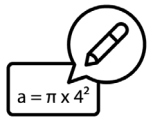
QR 4: DSGVO Art. 9,
Gesundheitsdaten



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

Weitere Quellen:

- Datenschutz-Notizen:
<https://www.datenschutz-notizen.de/die-vermessung-der-gesundheit-wie-positionieren-sich-krankenkassen-zu-wearables-1112189/>
- Datenschutzexperte.de:
<https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/datenschutz-im-gesundheitswesen/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/der-datenschutz-bei-krankenkassen/>



2. 2-Minuten Filmszene: Krankenkassen und Wearables

Szene-Titel:

„Deine Gesundheitsdaten unter Beobachtung“

Ort:

Ein Fitnessstudio, in dem Person A auf dem Laufband läuft und dabei ihr Fitness-Tracker-Armband trägt. Person B sitzt daneben auf einer Bank, schaut auf das Smartphone und spricht über Wearables.

Person A (läuft auf dem Laufband, schaut auf ihr Armband):

„Ich liebe meinen Tracker, er zeigt mir genau, wie viele Kalorien ich verbrannt habe und wie lange ich geschlafen habe.“

Person B (schaut neugierig auf ihr Smartphone):

„Ja, cool – aber weißt du, dass deine Krankenkasse diese Daten wahrscheinlich auch sehen kann?“

Person A (verwirrt):

„Was? Wie das?“

Person B (ernst):

„Viele Krankenkassen bieten Rabatte an, wenn du deinen Fitness-Tracker mit ihnen teilst. Sie nutzen die Daten, um zu sehen, ob du ein gesundes Leben führst – aber sie könnten sie auch nutzen, um deine Beiträge zu erhöhen, wenn du ungesund lebst.“

Person A (besorgt):

„Und wie sicher sind meine Daten dabei?“

Person B (erklärt):

„Gesundheitsdaten sind besonders geschützt durch die DSGVO. Die Daten sollten nur mit deiner Einwilligung genutzt werden. Aber der Algorithmus der Krankenkassen analysiert alles – und da ist immer das Risiko, dass die Daten gegen dich verwendet werden.“

Person A (entschlossen):

„Das ist echt beunruhigend. Ich werde mal nachsehen, welche Daten meine Krankenkasse von mir hat.“

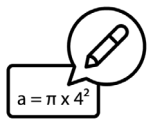
Schlusszene:

Text auf dem Bildschirm:

„Schütze deine Gesundheitsdaten. Informiere dich über deine Rechte. #DSGVO #BigData #Wearables #Krankenkasse“

Voiceover:

„Deine Daten sind wertvoll. Vergewissere dich, dass du sie im Griff hast.“



Was haben Krankenkassen mit meiner Smartwatch zu tun?

Krankenkassen und Wearables bieten ein anschauliches Beispiel für den Einsatz von Big Data im Gesundheitswesen. Wearables wie Fitness-Tracker, Smartwatches und andere vernetzte Geräte erfassen kontinuierlich Gesundheitsdaten wie Herzfrequenz, Schlafmuster, Bewegungsaktivität oder Kalorienverbrauch. Diese Daten können in Kombination mit Gesundheits-Apps und digitalen Plattformen gesammelt und ausgewertet werden.

Immer mehr Krankenkassen bieten Anreize an, um Versicherte dazu zu bewegen, ihre Wearable-Daten zu teilen. Ein Beispiel hierfür sind Bonusprogramme: Versicherte erhalten Prämien oder Vergünstigungen, wenn sie nachweisen, dass sie bestimmte Gesundheitsziele erreichen, wie z. B. eine bestimmte Anzahl von Schritten pro Tag oder das Einhalten eines Trainingsplans. Durch das Teilen dieser Daten sollen Versicherte zu einem gesünderen Lebensstil motiviert werden, was in der Theorie langfristig auch die Krankheitskosten senken könnte.

Allerdings gibt es bei dieser Praxis auch erhebliche Bedenken in Bezug auf den Datenschutz und die Privatsphäre. Die gesammelten Daten über Wearables sind sehr persönlich und können tiefgreifende Einblicke in den Gesundheitszustand, den Lebensstil und sogar potenzielle Risiken geben. Eine große Frage ist, ob Versicherte durch den „freiwilligen“ Datenaustausch Nachteile erleiden könnten. Wenn jemand nicht bereit ist, seine Gesundheitsdaten zu teilen, könnte das als Indiz dafür gewertet werden, dass diese Person etwas zu verbergen hat oder potenziell ein höheres Gesundheitsrisiko darstellt. Dies könnte langfristig zu Ungleichheiten in den Beitragszahlungen führen.

Die Datenschutz-Grundverordnung (DSGVO) der EU spielt auch hier eine zentrale Rolle. Versicherte müssen klar und transparent darüber informiert werden, welche Daten gesammelt werden, wie sie verwendet werden und wie lange sie gespeichert bleiben. Sie müssen auch ihre ausdrückliche Einwilligung zur Datennutzung geben. Allerdings stellt sich die Frage, ob diese Einwilligung tatsächlich freiwillig ist, wenn Versicherte spürbare Vorteile erhalten, wenn sie zustimmen – oder potenziell Nachteile haben, wenn sie ablehnen.

Ein weiterer Aspekt ist, dass die Wearable-Daten oft in Echtzeit gesammelt und ausgewertet werden, was den Versicherern ermöglicht, sofortige Rückschlüsse auf das Verhalten der Versicherten zu ziehen. Diese dynamischen Daten können dazu führen, dass Krankenkassen nicht nur rückblickend auf das Gesundheitsverhalten blicken, sondern auch zukünftige Risiken vorhersagen und darauf basierend Prämien oder Behandlungsstrategien anpassen.



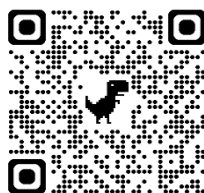
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die durch Wearables erhoben und bei der Krankenkasse gespeichert werden?
- Was passiert mit den Daten, die du durch Wearables wie Smartwatches und Fitness-Tracker teilst? Inwiefern sind diese Daten rechtlich geschützt?
- Welche Regeln der DSGVO/des Telemediengesetzes schützen dich davor, dass deine Wearable-Daten gegen dich verwendet werden?
- Wie kannst du sicherstellen, dass deine Wearable-Daten gelöscht werden? Recherchiere das „Recht auf Vergessenwerden“ in Bezug auf Krankenkassen und Gesundheitsdaten.

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Telemediengesetz



QR 4: DSGVO Art. 9,
Gesundheitsdaten



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

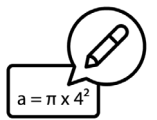


Weitere Quellen:

- Datenschutz-Notizen:
<https://www.datenschutz-notizen.de/die-vermessung-der-gesundheit-wie-positionieren-sich-krankenkassen-zu-wearables-1112189/>
- Datenschutzexperte.de:
<https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/datenschutz-im-gesundheitswesen/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/der-datenschutz-bei-krankenkassen/>



KRANKENKASSEN UND WEARABLES



Flyer-Design: „Schon gewusst?“ –Krankenkasse und Wearables (KI-generiert)

Layout:

1. **Größe des Flyers:** A5 (einseitig).
2. **Farbgestaltung:** Ein modernes, professionelles Design mit **Schattierungen von Grün und Weiß**. Grün steht für Gesundheit und Sicherheit, während Weiß für Sauberkeit und Lesbarkeit sorgt.

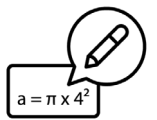
Flyer-Inhalt:

1. **Überschrift:**
 - **Position:** Oben auf dem Flyer, zentriert.
 - **Text:** „Schon gewusst?“ in **großer, fetter Schrift**.
 - **Schriftart:** Eine moderne, klare Schriftart (z.B. Arial oder Helvetica).
 - **Farbe:** **Grün**, um die Aufmerksamkeit zu erregen.
2. **Einleitender Text:**
 - **Position:** Direkt unter der Überschrift.
 - **Text:** Eine kurze Erklärung, die beschreibt, wie Krankenkassen Wearable-Daten sammeln und nutzen. Der Text sollte in einem kurzen Absatz zusammengefasst werden.
 - **Schriftart:** Etwas kleiner als die Überschrift, aber gut lesbar.
 - **Farbe:** **Schwarz** oder **dunkles Grau** für klare Lesbarkeit.
3. **Fakten und Tipps:**
 - **Position:** In der Mitte des Flyers, als **Liste** angeordnet.
 - **Text:** Eine Liste mit 3–4 Tipps zum Schutz der Gesundheitsdaten, z.B. „Überprüfe deine Datenschutz-Einstellungen“, „Nutze dein Recht auf Vergessenwerden“ und „Lies die Bedingungen deiner Krankenkasse“.
 - **Schriftart:** Leicht hervorgehoben (z.B. fett oder kursiv), damit die Tipps ins Auge fallen.
 - **Farbe:** **Schwarz** für den Text, mit **Grün** für Aufzählungspunkte oder Nummern, um die Liste hervorzuheben.
4. **Grafik/Symbol:**
 - **Position:** Unten rechts auf dem Flyer.
 - **Bild:** Eine einfache Darstellung eines **Wearable-Geräts** oder eines **Gesundheitsdaten-Symbols**.
 - **Größe:** Klein und dezent, damit es den Text nicht überlagert, aber das Thema visuell unterstreicht.
5. **Abschlussatz:**
 - **Position:** Unten links oder zentriert, neben der Grafik.
 - **Text:** „Bleib informiert und schütze deine Gesundheitsdaten. #DSGVO #Wearables #BigData“.
 - **Schriftart:** Klein und fein, aber gut lesbar.
 - **Farbe:** **Grün** oder **Grau**, um harmonisch zum Rest des Designs zu passen.



Gestaltungstipps:

- Nutzt **weißen Raum**, um den Flyer nicht zu überladen. Jeder Abschnitt sollte gut voneinander getrennt sein.
- **Symmetrie** hilft, das Design ordentlich und professionell wirken zu lassen.
- **Icons** oder kleine Grafiken können an den Rändern oder in der Mitte der Seite eingefügt werden, um den Flyer ansprechender zu gestalten.



Was haben Krankenkassen mit meiner Smartwatch zu tun?

Krankenkassen und Wearables bieten ein anschauliches Beispiel für den Einsatz von Big Data im Gesundheitswesen. Wearables wie Fitness-Tracker, Smartwatches und andere vernetzte Geräte erfassen kontinuierlich Gesundheitsdaten wie Herzfrequenz, Schlafmuster, Bewegungsaktivität oder Kalorienverbrauch. Diese Daten können in Kombination mit Gesundheits-Apps und digitalen Plattformen gesammelt und ausgewertet werden.

Immer mehr Krankenkassen bieten Anreize an, um Versicherte dazu zu bewegen, ihre Wearable-Daten zu teilen. Ein Beispiel hierfür sind Bonusprogramme: Versicherte erhalten Prämien oder Vergünstigungen, wenn sie nachweisen, dass sie bestimmte Gesundheitsziele erreichen, wie z. B. eine bestimmte Anzahl von Schritten pro Tag oder das Einhalten eines Trainingsplans. Durch das Teilen dieser Daten sollen Versicherte zu einem gesünderen Lebensstil motiviert werden, was in der Theorie langfristig auch die Krankheitskosten senken könnte.

Allerdings gibt es bei dieser Praxis auch erhebliche Bedenken in Bezug auf den Datenschutz und die Privatsphäre. Die gesammelten Daten über Wearables sind sehr persönlich und können tiefgreifende Einblicke in den Gesundheitszustand, den Lebensstil und sogar potenzielle Risiken geben. Eine große Frage ist, ob Versicherte durch den „freiwilligen“ Datenaustausch Nachteile erleiden könnten. Wenn jemand nicht bereit ist, seine Gesundheitsdaten zu teilen, könnte das als Indiz dafür gewertet werden, dass diese Person etwas zu verbergen hat oder potenziell ein höheres Gesundheitsrisiko darstellt. Dies könnte langfristig zu Ungleichheiten in den Beitragszahlungen führen.

Die Datenschutz-Grundverordnung (DSGVO) der EU spielt auch hier eine zentrale Rolle. Versicherte müssen klar und transparent darüber informiert werden, welche Daten gesammelt werden, wie sie verwendet werden und wie lange sie gespeichert bleiben. Sie müssen auch ihre ausdrückliche Einwilligung zur Datennutzung geben. Allerdings stellt sich die Frage, ob diese Einwilligung tatsächlich freiwillig ist, wenn Versicherte spürbare Vorteile erhalten, wenn sie zustimmen – oder potenziell Nachteile haben, wenn sie ablehnen.

Ein weiterer Aspekt ist, dass die Wearable-Daten oft in Echtzeit gesammelt und ausgewertet werden, was den Versicherern ermöglicht, sofortige Rückschlüsse auf das Verhalten der Versicherten zu ziehen. Diese dynamischen Daten können dazu führen, dass Krankenkassen nicht nur rückblickend auf das Gesundheitsverhalten blicken, sondern auch zukünftige Risiken vorhersagen und darauf basierend Prämien oder Behandlungsstrategien anpassen.



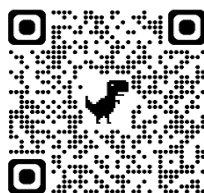
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wem gehören die Daten, die durch Wearables erhoben und bei der Krankenkasse gespeichert werden?
- Was passiert mit den Daten, die du durch Wearables wie Smartwatches und Fitness-Tracker teilst? Inwiefern sind diese Daten rechtlich geschützt?
- Welche Regeln der DSGVO/des Telemediengesetzes schützen dich davor, dass deine Wearable-Daten gegen dich verwendet werden?
- Wie kannst du sicherstellen, dass deine Wearable-Daten gelöscht werden? Recherchiere das „Recht auf Vergessenwerden“ in Bezug auf Krankenkassen und Gesundheitsdaten.

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Telemediengesetz



QR 4: DSGVO Art. 9,
Gesundheitsdaten

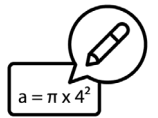


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- Datenschutz-Notizen:
<https://www.datenschutz-notizen.de/die-vermessung-der-gesundheit-wie-positionieren-sich-krankenkassen-zu-wearables-1112189/>
- Datenschutzexperte.de:
<https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/datenschutz-im-gesundheitswesen/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/der-datenschutz-bei-krankenkassen/>



4. Social-Media-Kampagne: Krankenkassen und Wearables

3 Beiträge der Kampagne:

Beitrag 1: Podcast-Ankündigung

- **Bild/Video:** Ein animiertes Bild mit dem Titel „Krankenkassen und Wearables: Was du wissen musst“ und einem Play-Button.
- **Text (Post-Beschreibung):**
„👂 Wie viel weiß deine Krankenkasse über deine Gesundheit? Erfahre in unserem neuen Podcast, wie deine Wearable-Daten verwendet werden und welche Risiken es gibt.
👉 Hör jetzt rein!
#Wearables #Gesundheitsdaten #DSGVO #Krankenkasse“

Beitrag 2: 2-Minuten-Video „Deine Gesundheitsdaten unter Beobachtung“

- **Bild/Video:** Das 2-minütige Video, das eine Unterhaltung über Krankenkassen und Wearables zeigt.
- **Text (Post-Beschreibung):** „👁️ Was macht deine Krankenkasse mit deinen Gesundheitsdaten? Erfahre in unserem neuen Video, welche Daten gesammelt werden und wie du dich schützen kannst! #Wearables #Datenschutz #DSGVO #BigData“

Beitrag 3: Aufklärungsflyer

- **Bild:** Der Flyer über Wearables und Datenschutz.
- **Text (Post-Beschreibung):** „📄 Hol dir unseren Flyer und erfahre, wie du deine Wearable-Daten vor Missbrauch schützen kannst! #Flyer #Datenschutz #DSGVO #Wearables“

Post-Idee 1: Quiz zur Wearable-Datensicherheit

- **Bild:** Ein interaktives Bild mit der Quiz-Frage: „Wusstest du, dass deine Krankenkasse deine Fitnessdaten sehen kann?“ mit Antwortmöglichkeiten wie: „Ja, aber mir egal!“ oder „Nein, das ist mir neu!“.
- **Text:** „Teste dein Wissen! Weißt du, wie deine Wearable-Daten genutzt werden? Nimm an unserem Quiz teil und finde es heraus! #Datenschutz #Wearables #Quiz #DSGVO“

Post-Idee 2: Fakten über Wearables und Krankenkassen

- **Bild:** Eine Infografik mit Fakten zu Krankenkassen und Wearable-Daten, z.B. „Gesundheitsdaten sind besonders schützenswert! Krankenkassen nutzen diese Daten, um Präventionsprogramme zu erstellen – aber was passiert, wenn die Daten missbraucht werden?“.
- **Text:** „Schon gewusst? Krankenkassen können deine Fitness- und Gesundheitsdaten nutzen, um dich zu bewerten. Erfahre, wie du deine Daten schützen kannst! #Wearables #Datensicherheit #Krankenkassen #DSGVO“

Story-Idee: Umfrage zu Wearables und Datenschutz

- **Frage:** „Nutzt du Wearables (z.B. Smartwatches, Fitness-Tracker)? Weißt du, wer Zugriff auf deine Daten hat?“
- **Optionen:** „Ja, ich passe auf!“ / „Nein, keine Ahnung!“
- **Ergebnis:** Bei „Nein“ könnte ein Swipe-up-Link zu einem erklärenden Video oder einem Infopost geleitet werden.

Post-Idee 3: Tutorial zum Datenschutz bei Wearables

- **Bild:** Ein Bild von einem Fitness-Tracker oder einer Smartwatch, mit einem Datenschutz-Symbol daneben.
- **Text:**
„Deine Fitnessdaten sind wertvoll – auch für Krankenkassen! Erfahre in unserem Tutorial, wie du die Datenschutzeinstellungen deines Wearables anpassen kannst, um deine Daten zu schützen.
#Wearables #Datenschutz #DSGVO #SicherimNetz“

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

PERSONALISIERTE WERBUNG

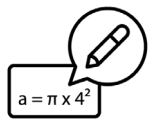
Personalisierte Werbung hat jeden schon mal getroffen: du scrollst auf Instagram oder auf einer Nachrichten-Seite herum und plötzlich wird dir eine Werbung zu einem Produkt angezeigt, dass du gerade noch im Web gesucht hast. Doch ist dir eigentlich bewusst, dass die Mechanismen der personalisierten Werbung auch für Nachrichtenartikel und politische Anzeigen funktionieren? Cookies tracken dein Verhalten und auf deren Basis zeigen dir Werbende das, was dich interessiert. Im Präsidentschaftswahlkampf Trumps wurde diese Microtagging-Strategie verwendet und im Nachhinein in der Presse als Wahlbeeinflussung betitelt. Welche Auswirkung hat also personalisierte Werbung?

PODCAST

Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



Hast du auch personalisierte Werbung in deinem Feed?

Personalisierte Werbung auf Social Media ist ein Mechanismus, bei dem Nutzerdaten verwendet werden, um individuelle Werbeanzeigen zu schalten. Plattformen wie Facebook, Instagram oder TikTok setzen komplexe Algorithmen ein, um das Verhalten von Nutzern zu analysieren. Jedes „Gefällt mir“, jeder Kommentar, jede Suchanfrage und sogar die Zeit, die du mit bestimmten Inhalten verbringst, wird verfolgt und gespeichert. Diese Daten ermöglichen es Plattformen, personalisierte Profile zu erstellen, die dann an Werbetreibende weitergegeben werden. Diese können ihre Anzeigen gezielt auf Nutzer zuschneiden, die am wahrscheinlichsten auf ihre Produkte reagieren. Ein zentraler Bestandteil dieser Datenerhebung sind **Cookies**. Cookies sind kleine Textdateien, die auf deinem Gerät gespeichert werden, wenn du eine Website besuchst. Sie dienen in erster Linie dazu, Informationen über dein Surfverhalten zu speichern, wie beispielsweise Login-Informationen, aber auch, welche Seiten du besuchst, wie lange du auf einer Seite verweilst und welche Produkte du anschaust. Durch den Einsatz von Cookies können Plattformen und Werbetreibende ein detailliertes Bild deines Online-Verhaltens erstellen. Hast du dich jemals gefragt, warum du auf fast jeder Website gefragt wirst, ob du Cookies akzeptieren möchtest? Das hat zwei Gründe: Erstens sind Cookies ein zentrales Element, um dein Erlebnis auf Websites angenehmer zu gestalten – sie merken sich z.B. deine Spracheinstellungen oder deinen Warenkorb in Online-Shops. Zweitens ermöglichen sie aber auch das Tracking deines Surfverhaltens. Durch Cookies können Werbenetzwerke über mehrere Seiten hinweg verfolgen, welche Inhalte du anschaust, um dir später gezielte Werbung anzuzeigen. **Die Datenschutz-Grundverordnung (DSGVO)** der EU hat hier einen wichtigen Schutzmechanismus eingeführt: Websites müssen die Zustimmung der Nutzer zur Verwendung von Cookies einholen, bevor sie diese einsetzen dürfen. Du hast also die Wahl, Cookies zu akzeptieren oder abzulehnen. Allerdings sind die meisten Cookies, insbesondere die sogenannten "Tracking-Cookies", darauf ausgelegt, Informationen über dich zu sammeln, um dich für personalisierte Werbung besser zu targetieren. **Das Problem:** Obwohl die DSGVO Nutzern mehr Kontrolle über ihre Daten gibt, ist die Realität oft undurchsichtig. Viele Nutzer wissen nicht genau, welche Daten durch Cookies und andere Tracking-Methoden gesammelt werden, und oft ist es schwierig, die vollständige Kontrolle über diese Informationen zu erlangen. Auch das Löschen von Cookies oder das Deaktivieren bestimmter Tracking-Funktionen schränkt die Überwachung oft nur geringfügig ein, da viele Websites auf Cookies angewiesen sind, um personalisierte Werbung zu ermöglichen. **Zusammengefasst:** Personalisierte Werbung hat den Vorteil, dass du relevantere Inhalte siehst. Doch sie birgt auch erhebliche Risiken für deine Privatsphäre, insbesondere, wenn du nicht weißt, wie viele Daten über dich gesammelt werden und wie tief die Überwachung durch Cookies und andere Tracking-Technologien geht. Zum Glück bietet die DSGVO Schutz, indem sie den Nutzern das Recht auf Information, Auskunft und Löschung ihrer Daten gibt.

Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Welche Daten werden von Social Media-Plattformen gesammelt, um personalisierte Werbung zu schalten? Was regelt die DSGVO hierzu?
- Was sind Cookies und wie funktionieren sie? Was haben sie mit der Datensammlung zu tun?
- Welche Regeln der DSGVO/BMUV schützen dich vor unkontrollierter Datennutzung?
- Wie beeinflusst personalisierte Werbung die Privatsphäre? Was ist der „Klarnamenzwang“ und was hat er damit zu tun?
- Welche Chancen und Risiken entstehen durch personalisierte Werbung bzw. personalisierter Inhalte?

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



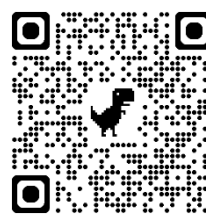
QR 1: BMUV über Cookies und personalisierte Werbung



QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: DSGVO Art. 21, Widerspruchsrecht



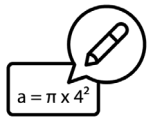
QR 4: DSGVO Art. 15, Auskunftsrecht



QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

Weitere Quellen:

- Basicthinking.de: <https://www.basicthinking.de/blog/2021/08/24/personalisierte-werbung-gorelate/>
- Welivesecurity.com: <https://www.welivesecurity.com/deutsch/2021/09/09/hungrige-datenkraken-welche-daten-sammeln-facebook-co-ueber-uns/>
- BMUV: <https://www.bmuv.de/themen/verbraucherschutz/digitaler-verbraucherschutz/personalisierte-werbung-und-tracking>
- Dr. Datenschutz: <https://www.dr-datenschutz.de/social-media-darf-man-die-oeffentlich-zugaenglichen-daten-nutzen/>



1. Podcast-Interviewer-Leitfaden (5-Minuten Podcast)

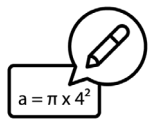
Erstelle einen 5-Minuten-Podcast

Thema: „Personalisierte Werbung auf Social Media: Wie Cookies unsere Privatsphäre gefährden“

1. Einleitung:
„Willkommen zu unserem Podcast! Heute geht es um personalisierte Werbung und wie Plattformen wie Facebook und Instagram Cookies verwenden, um unsere Daten zu sammeln und uns gezielt Werbung anzuzeigen. Aber was bedeutet das für unsere Privatsphäre?“
2. Frage 1:
„Was ist personalisierte Werbung und wie funktioniert sie auf Social Media?“
(Ziel: Eine Einführung in die Welt der personalisierten Werbung, wie sie durch das Sammeln von Daten individualisierte Anzeigen schaltet.)
3. Frage 2:
„Was sind Cookies und warum werden sie auf so vielen Websites verwendet?“
(Ziel: Erkläre, was Cookies sind, wie sie Informationen speichern und wie sie zur Schaltung von personalisierter Werbung verwendet werden.)
4. Frage 3:
„Welche Daten werden durch Cookies gesammelt und wie nutzen Unternehmen diese Daten?“
(Ziel: Erkläre, welche Arten von Daten (z. B. Standort, Verweildauer auf Seiten, Kaufverhalten) über Cookies gesammelt werden und wie sie zur Erstellung von Werbeprofilen genutzt werden.)
5. Frage 4:
„Welche rechtlichen Schutzmechanismen gibt es, um die Privatsphäre der Nutzer zu schützen?“
(Ziel: Erläutere, wie die DSGVO versucht, die Datensammlung durch Cookies zu regulieren und welche Rechte Nutzer haben, um ihre Daten zu schützen.)
6. Frage 5:
„Wie können sich Nutzer vor unerwünschtem Tracking durch Cookies schützen?“
(Ziel: Biete praktische Tipps an, wie Nutzer Tracking-Cookies vermeiden, die Privatsphäre-Einstellungen anpassen und Tracking-Blocker nutzen können.)

Abschluss:

Fasst die wichtigsten Punkte zusammen und erklärt, wie Nutzer ihre Rechte in Bezug auf Cookies und personalisierte Werbung durchsetzen können.



Hast du auch personalisierte Werbung in deinem Feed?

Personalisierte Werbung auf Social Media ist ein Mechanismus, bei dem Nutzerdaten verwendet werden, um individuelle Werbeanzeigen zu schalten. Plattformen wie Facebook, Instagram oder TikTok setzen komplexe Algorithmen ein, um das Verhalten von Nutzern zu analysieren. Jedes „Gefällt mir“, jeder Kommentar, jede Suchanfrage und sogar die Zeit, die du mit bestimmten Inhalten verbringst, wird verfolgt und gespeichert. Diese Daten ermöglichen es Plattformen, personalisierte Profile zu erstellen, die dann an Werbetreibende weitergegeben werden. Diese können ihre Anzeigen gezielt auf Nutzer zuschneiden, die am wahrscheinlichsten auf ihre Produkte reagieren. Ein zentraler Bestandteil dieser Datenerhebung sind **Cookies**. Cookies sind kleine Textdateien, die auf deinem Gerät gespeichert werden, wenn du eine Website besuchst. Sie dienen in erster Linie dazu, Informationen über dein Surfverhalten zu speichern, wie beispielsweise Login-Informationen, aber auch, welche Seiten du besuchst, wie lange du auf einer Seite verweilst und welche Produkte du anschaust. Durch den Einsatz von Cookies können Plattformen und Werbetreibende ein detailliertes Bild deines Online-Verhaltens erstellen. Hast du dich jemals gefragt, warum du auf fast jeder Website gefragt wirst, ob du Cookies akzeptieren möchtest? Das hat zwei Gründe: Erstens sind Cookies ein zentrales Element, um dein Erlebnis auf Websites angenehmer zu gestalten – sie merken sich z.B. deine Spracheinstellungen oder deinen Warenkorb in Online-Shops. Zweitens ermöglichen sie aber auch das Tracking deines Surfverhaltens. Durch Cookies können Werbenetzwerke über mehrere Seiten hinweg verfolgen, welche Inhalte du anschaust, um dir später gezielte Werbung anzuzeigen. **Die Datenschutz-Grundverordnung (DSGVO)** der EU hat hier einen wichtigen Schutzmechanismus eingeführt: Websites müssen die Zustimmung der Nutzer zur Verwendung von Cookies einholen, bevor sie diese einsetzen dürfen. Du hast also die Wahl, Cookies zu akzeptieren oder abzulehnen. Allerdings sind die meisten Cookies, insbesondere die sogenannten "Tracking-Cookies", darauf ausgelegt, Informationen über dich zu sammeln, um dich für personalisierte Werbung besser zu targetieren. **Das Problem:** Obwohl die DSGVO Nutzern mehr Kontrolle über ihre Daten gibt, ist die Realität oft undurchsichtig. Viele Nutzer wissen nicht genau, welche Daten durch Cookies und andere Tracking-Methoden gesammelt werden, und oft ist es schwierig, die vollständige Kontrolle über diese Informationen zu erlangen. Auch das Löschen von Cookies oder das Deaktivieren bestimmter Tracking-Funktionen schränkt die Überwachung oft nur geringfügig ein, da viele Websites auf Cookies angewiesen sind, um personalisierte Werbung zu ermöglichen. **Zusammengefasst:** Personalisierte Werbung hat den Vorteil, dass du relevantere Inhalte siehst. Doch sie birgt auch erhebliche Risiken für deine Privatsphäre, insbesondere, wenn du nicht weißt, wie viele Daten über dich gesammelt werden und wie tief die Überwachung durch Cookies und andere Tracking-Technologien geht. Zum Glück bietet die DSGVO Schutz, indem sie den Nutzern das Recht auf Information, Auskunft und Löschung ihrer Daten gibt.

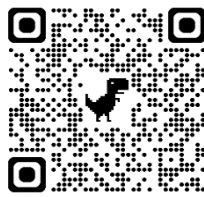
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Welche Daten werden von Social Media-Plattformen gesammelt, um personalisierte Werbung zu schalten? Was regelt die DSGVO hierzu?
- Was sind Cookies und wie funktionieren sie? Was haben sie mit der Datensammlung zu tun?
- Welche Regeln der DSGVO/BMUV schützen dich vor unkontrollierter Datennutzung?
- Wie beeinflusst personalisierte Werbung die Privatsphäre? Was ist der „Klarnamenzwang“ und was hat er damit zu tun?
- Welche Chancen und Risiken entstehen durch personalisierte Werbung bzw. personalisierter Inhalte?

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, das alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze iMovie/Clips zum Erstellen und Bearbeiten der Inhalte.



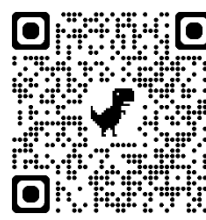
QR 1: BMUV über Cookies und personalisierte Werbung



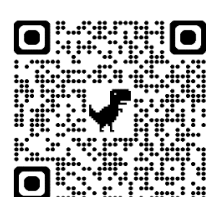
QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: DSGVO Art. 21, Widerspruchsrecht



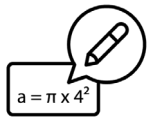
QR 4: DSGVO Art. 15, Auskunftsrecht



QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

Weitere Quellen:

- Basicthinking.de: <https://www.basicthinking.de/blog/2021/08/24/personalisierte-werbung-gorelate/>
- Welivesecurity.com: <https://www.welivesecurity.com/deutsch/2021/09/09/hungrige-datenkraken-welche-daten-sammeln-facebook-co-ueber-uns/>
- BMUV: <https://www.bmuv.de/themen/verbraucherschutz/digitaler-verbraucherschutz/personalisierte-werbung-und-tracking>
- Dr. Datenschutz: <https://www.dr-datenschutz.de/social-media-darf-man-die-oeffentlich-zugaenglichen-daten-nutzen/>



Szenenbeschreibung für ein 2-Minuten-Video

Titel: „Cookies und personalisierte Werbung: Wie du überall verfolgt wirst“

Ort: Ein gemütliches Wohnzimmer. Person A sitzt auf der Couch mit einem Laptop auf dem Schoß und scrollt durch verschiedene Online-Shops. Neben ihr sitzt Person B, die neugierig zuschaut.

Person A (genervt): „Jedes Mal, wenn ich eine Seite öffne, fragen die mich, ob ich Cookies akzeptiere. Was soll das eigentlich?“

Person B (wissend): „Das sind Cookies. Sie verfolgen, was du auf den Seiten machst, und speichern deine Daten, damit du beim nächsten Besuch nicht alles neu einstellen musst. Aber sie werden auch für Werbung genutzt.“

Person A (nachdenklich): „Also speichern die alles, was ich mir anschau?“

Person B (ernst): „Ja, und diese Daten werden dann genutzt, um dir gezielt Werbung anzuzeigen. Deswegen siehst du nach dem Besuch eines Online-Shops plötzlich überall Anzeigen für genau die Produkte, die du dir angesehen hast.“

Person A (besorgt): „Das ist ja fast wie Spionage. Wie kann ich das verhindern?“

Person B (beruhigend): „Du kannst zumindest teilweise kontrollieren, welche Cookies gespeichert werden. Aber die DSGVO verlangt zumindest, dass du informiert wirst und zustimmen musst, bevor Cookies verwendet werden.“

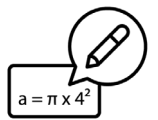
Person A (entschlossen): „Das klingt so, als müsste ich meine Einstellungen mal überprüfen.“

Schlusszene:

Text auf dem Bildschirm: „Schütze deine Privatsphäre. Erfahre, wie du Cookies und Tracking kontrollieren kannst.“

#DSGVO #Cookies #PersonalisierteWerbung

Voiceover: „Lerne, wie du deine Daten schützt. Es liegt in deiner Hand.“



Hast du auch personalisierte Werbung in deinem Feed?

Personalisierte Werbung auf Social Media ist ein Mechanismus, bei dem Nutzerdaten verwendet werden, um individuelle Werbeanzeigen zu schalten. Plattformen wie Facebook, Instagram oder TikTok setzen komplexe Algorithmen ein, um das Verhalten von Nutzern zu analysieren. Jedes „Gefällt mir“, jeder Kommentar, jede Suchanfrage und sogar die Zeit, die du mit bestimmten Inhalten verbringst, wird verfolgt und gespeichert. Diese Daten ermöglichen es Plattformen, personalisierte Profile zu erstellen, die dann an Werbetreibende weitergegeben werden. Diese können ihre Anzeigen gezielt auf Nutzer zuschneiden, die am wahrscheinlichsten auf ihre Produkte reagieren. Ein zentraler Bestandteil dieser Datenerhebung sind **Cookies**. Cookies sind kleine Textdateien, die auf deinem Gerät gespeichert werden, wenn du eine Website besuchst. Sie dienen in erster Linie dazu, Informationen über dein Surfverhalten zu speichern, wie beispielsweise Login-Informationen, aber auch, welche Seiten du besuchst, wie lange du auf einer Seite verweilst und welche Produkte du anschaust. Durch den Einsatz von Cookies können Plattformen und Werbetreibende ein detailliertes Bild deines Online-Verhaltens erstellen. Hast du dich jemals gefragt, warum du auf fast jeder Website gefragt wirst, ob du Cookies akzeptieren möchtest? Das hat zwei Gründe: Erstens sind Cookies ein zentrales Element, um dein Erlebnis auf Websites angenehmer zu gestalten – sie merken sich z.B. deine Spracheinstellungen oder deinen Warenkorb in Online-Shops. Zweitens ermöglichen sie aber auch das Tracking deines Surfverhaltens. Durch Cookies können Werbenetzwerke über mehrere Seiten hinweg verfolgen, welche Inhalte du anschaust, um dir später gezielte Werbung anzuzeigen. **Die Datenschutz-Grundverordnung (DSGVO)** der EU hat hier einen wichtigen Schutzmechanismus eingeführt: Websites müssen die Zustimmung der Nutzer zur Verwendung von Cookies einholen, bevor sie diese einsetzen dürfen. Du hast also die Wahl, Cookies zu akzeptieren oder abzulehnen. Allerdings sind die meisten Cookies, insbesondere die sogenannten "Tracking-Cookies", darauf ausgelegt, Informationen über dich zu sammeln, um dich für personalisierte Werbung besser zu targetieren. **Das Problem:** Obwohl die DSGVO Nutzern mehr Kontrolle über ihre Daten gibt, ist die Realität oft undurchsichtig. Viele Nutzer wissen nicht genau, welche Daten durch Cookies und andere Tracking-Methoden gesammelt werden, und oft ist es schwierig, die vollständige Kontrolle über diese Informationen zu erlangen. Auch das Löschen von Cookies oder das Deaktivieren bestimmter Tracking-Funktionen schränkt die Überwachung oft nur geringfügig ein, da viele Websites auf Cookies angewiesen sind, um personalisierte Werbung zu ermöglichen. **Zusammengefasst:** Personalisierte Werbung hat den Vorteil, dass du relevantere Inhalte siehst. Doch sie birgt auch erhebliche Risiken für deine Privatsphäre, insbesondere, wenn du nicht weißt, wie viele Daten über dich gesammelt werden und wie tief die Überwachung durch Cookies und andere Tracking-Technologien geht. Zum Glück bietet die DSGVO Schutz, indem sie den Nutzern das Recht auf Information, Auskunft und Löschung ihrer Daten gibt.

Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Welche Daten werden von Social Media-Plattformen gesammelt, um personalisierte Werbung zu schalten? Was regelt die DSGVO hierzu?
- Was sind Cookies und wie funktionieren sie? Was haben sie mit der Datensammlung zu tun?
- Welche Regeln der DSGVO/BMUV schützen dich vor unkontrollierter Datennutzung?
- Wie beeinflusst personalisierte Werbung die Privatsphäre? Was ist der „Klarnamenzwang“ und was hat er damit zu tun?
- Welche Chancen und Risiken entstehen durch personalisierte Werbung bzw. personalisierter Inhalte?

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



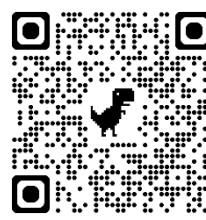
QR 1: BMUV über Cookies und personalisierte Werbung



QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: DSGVO Art. 21, Widerspruchsrecht



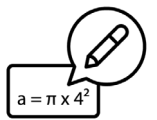
QR 4: DSGVO Art. 15, Auskunftsrecht



QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

Weitere Quellen:

- Basicthinking.de: <https://www.basicthinking.de/blog/2021/08/24/personalisierte-werbung-gorelate/>
- Welivesecurity.com: <https://www.welivesecurity.com/deutsch/2021/09/09/hungrige-datenkraken-welche-daten-sammeln-facebook-co-ueber-uns/>
- BMUV: <https://www.bmuv.de/themen/verbraucherschutz/digitaler-verbraucherschutz/personalisierte-werbung-und-tracking>
- Dr. Datenschutz: <https://www.dr-datenschutz.de/social-media-darf-man-die-oeffentlich-zugaenglichen-daten-nutzen/>



Flyer-Design: „Schon gewusst?“ – Personalisierte Werbung und Cookies (KI-generiert)

Layout:

1. Größe des Flyers: A5 (einseitig).
2. Farbgestaltung: Ein modernes, professionelles Design mit Schattierungen von Blau und Weiß. Blau steht für Technologie und Transparenz, während Weiß für Sauberkeit und Lesbarkeit sorgt.

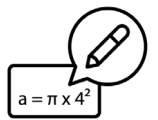
Flyer-Inhalt:

1. Überschrift:
 - Position: Oben auf dem Flyer, zentriert.
 - Text: „Schon gewusst?“ in großer, fetter Schrift.
 - Schriftart: Eine moderne, klare Schriftart (z.B. Arial oder Helvetica).
 - Farbe: Blau, um die Aufmerksamkeit zu erregen.
2. Einleitender Text:
 - Position: Direkt unter der Überschrift.
 - Text: Eine kurze Erklärung, die beschreibt, wie Social Media-Plattformen Cookies verwenden, um dein Online-Verhalten zu verfolgen und personalisierte Werbung zu schalten. Der Text sollte in einem kurzen Absatz zusammengefasst werden.
 - Schriftart: Etwas kleiner als die Überschrift, aber gut lesbar.
 - Farbe: Schwarz oder dunkles Grau für klare Lesbarkeit.
3. Fakten und Tipps:
 - Position: In der Mitte des Flyers, als Liste angeordnet.
 - Text: Eine Liste mit 3–4 Tipps, wie du dich vor ungewolltem Tracking und personalisierter Werbung schützen kannst, z.B. „Überprüfe deine Cookie-Einstellungen“, „Nutze den Inkognito-Modus“, „Fordere deine Daten gemäß DSGVO an“.
 - Schriftart: Leicht hervorgehoben (z.B. fett oder kursiv), damit die Tipps ins Auge fallen.
 - Farbe: Schwarz für den Text, mit Blau für Aufzählungspunkte oder Nummern, um die Liste hervorzuheben.
4. Grafik/Symbol:
 - Position: Unten rechts auf dem Flyer.
 - Bild: Eine einfache Darstellung eines Cookie-Symbols oder eines Datenschutzeschildes.
 - Größe: Klein und dezent, damit es den Text nicht überlagert, aber das Thema visuell unterstreicht.
5. Abschlusssatz:
 - Position: Unten links oder zentriert, neben der Grafik.
 - Text: „Bleib informiert und schütze deine Daten. #DSGVO #PersonalisierteWerbung #Cookies“.
 - Schriftart: Klein und fein, aber gut lesbar.
 - Farbe: Blau oder Grau, um harmonisch zum Rest des Designs zu passen.



Gestaltungstipps:

- Nutze weißen Raum, um den Flyer nicht zu überladen. Jeder Abschnitt sollte gut voneinander getrennt sein.
- Symmetrie hilft, das Design ordentlich und professionell wirken zu lassen.
- Icons oder kleine Grafiken können an den Rändern oder in der Mitte der Seite eingefügt werden, um den Flyer ansprechender zu gestalten.



Hast du auch personalisierte Werbung in deinem Feed?

Personalisierte Werbung auf Social Media ist ein Mechanismus, bei dem Nutzerdaten verwendet werden, um individuelle Werbeanzeigen zu schalten. Plattformen wie Facebook, Instagram oder TikTok setzen komplexe Algorithmen ein, um das Verhalten von Nutzern zu analysieren. Jedes „Gefällt mir“, jeder Kommentar, jede Suchanfrage und sogar die Zeit, die du mit bestimmten Inhalten verbringst, wird verfolgt und gespeichert. Diese Daten ermöglichen es Plattformen, personalisierte Profile zu erstellen, die dann an Werbetreibende weitergegeben werden. Diese können ihre Anzeigen gezielt auf Nutzer zuschneiden, die am wahrscheinlichsten auf ihre Produkte reagieren. Ein zentraler Bestandteil dieser Datenerhebung sind **Cookies**. Cookies sind kleine Textdateien, die auf deinem Gerät gespeichert werden, wenn du eine Website besuchst. Sie dienen in erster Linie dazu, Informationen über dein Surfverhalten zu speichern, wie beispielsweise Login-Informationen, aber auch, welche Seiten du besuchst, wie lange du auf einer Seite verweilst und welche Produkte du anschaust. Durch den Einsatz von Cookies können Plattformen und Werbetreibende ein detailliertes Bild deines Online-Verhaltens erstellen. Hast du dich jemals gefragt, warum du auf fast jeder Website gefragt wirst, ob du Cookies akzeptieren möchtest? Das hat zwei Gründe: Erstens sind Cookies ein zentrales Element, um dein Erlebnis auf Websites angenehmer zu gestalten – sie merken sich z.B. deine Spracheinstellungen oder deinen Warenkorb in Online-Shops. Zweitens ermöglichen sie aber auch das Tracking deines Surfverhaltens. Durch Cookies können Werbenetzwerke über mehrere Seiten hinweg verfolgen, welche Inhalte du anschaust, um dir später gezielte Werbung anzuzeigen. **Die Datenschutz-Grundverordnung (DSGVO)** der EU hat hier einen wichtigen Schutzmechanismus eingeführt: Websites müssen die Zustimmung der Nutzer zur Verwendung von Cookies einholen, bevor sie diese einsetzen dürfen. Du hast also die Wahl, Cookies zu akzeptieren oder abzulehnen. Allerdings sind die meisten Cookies, insbesondere die sogenannten "Tracking-Cookies", darauf ausgelegt, Informationen über dich zu sammeln, um dich für personalisierte Werbung besser zu targetieren. **Das Problem:** Obwohl die DSGVO Nutzern mehr Kontrolle über ihre Daten gibt, ist die Realität oft undurchsichtig. Viele Nutzer wissen nicht genau, welche Daten durch Cookies und andere Tracking-Methoden gesammelt werden, und oft ist es schwierig, die vollständige Kontrolle über diese Informationen zu erlangen. Auch das Löschen von Cookies oder das Deaktivieren bestimmter Tracking-Funktionen schränkt die Überwachung oft nur geringfügig ein, da viele Websites auf Cookies angewiesen sind, um personalisierte Werbung zu ermöglichen. **Zusammengefasst:** Personalisierte Werbung hat den Vorteil, dass du relevantere Inhalte siehst. Doch sie birgt auch erhebliche Risiken für deine Privatsphäre, insbesondere, wenn du nicht weißt, wie viele Daten über dich gesammelt werden und wie tief die Überwachung durch Cookies und andere Tracking-Technologien geht. Zum Glück bietet die DSGVO Schutz, indem sie den Nutzern das Recht auf Information, Auskunft und Löschung ihrer Daten gibt.

Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Welche Daten werden von Social Media-Plattformen gesammelt, um personalisierte Werbung zu schalten? Was regelt die DSGVO hierzu?
- Was sind Cookies und wie funktionieren sie? Was haben sie mit der Datensammlung zu tun?
- Welche Regeln der DSGVO/BMUV schützen dich vor unkontrollierter Datennutzung?
- Wie beeinflusst personalisierte Werbung die Privatsphäre? Was ist der „Klarnamenzwang“ und was hat er damit zu tun?
- Welche Chancen und Risiken entstehen durch personalisierte Werbung bzw. personalisierter Inhalte?

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



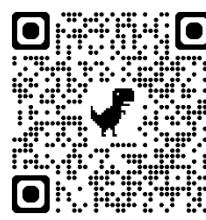
QR 1: BMUV über Cookies und personalisierte Werbung



QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: DSGVO Art. 21, Widerspruchsrecht



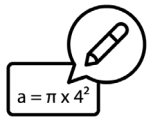
QR 4: DSGVO Art. 15, Auskunftsrecht



QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

Weitere Quellen:

- Basicthinking.de: <https://www.basicthinking.de/blog/2021/08/24/personalisierte-werbung-gorelate/>
- Welivesecurity.com: <https://www.welivesecurity.com/deutsch/2021/09/09/hungrige-datenkraken-welche-daten-sammeln-facebook-co-ueber-uns/>
- BMUV: <https://www.bmuv.de/themen/verbraucherschutz/digitaler-verbraucherschutz/personalisierte-werbung-und-tracking>
- Dr. Datenschutz: <https://www.dr-datenschutz.de/social-media-darf-man-die-oeffentlich-zugaenglichen-daten-nutzen/>



Social-Media-Kampagne: Personalisierte Werbung und Cookies

Instagram-Profil-Name: „@DatenschutzCookies“

Profil-Beschreibung (Bio): „Schütze deine Daten vor personalisierter Werbung! Erfahre, wie Social Media Cookies verwendet und welche Auswirkungen das auf deine Privatsphäre hat. 🎧 Podcast | 📺 Video | 📄 Flyer“

Profilbild: Ein Symbol, das ein Cookie und ein Datenschutz-Schild kombiniert.

3 Beiträge der Kampagne:

Beitrag 1: Podcast-Ankündigung

- Bild/Video: Ein animiertes Bild mit dem Titel „Personalisierte Werbung: Was du wissen musst“ und einem Play-Button.
- Text (Post-Beschreibung): „🎧 Erfahre in unserem neuen Podcast, wie Social Media Cookies verwendet, um dein Online-Verhalten zu verfolgen, und welche Folgen das für deine Privatsphäre hat. ➡ Hör jetzt rein! #Cookies #PersonalisierteWerbung #DSGVO #Privatsphäre“

Beitrag 2: 2-Minuten-Video „Deine Daten unter Beobachtung“

- Bild/Video: Ein 2-minütiges Video, das eine Unterhaltung über die Verwendung von Cookies und personalisierter Werbung auf Social Media zeigt.
- Text (Post-Beschreibung): „👁️ Weißt du, wie viel Social Media über dich weiß? Unser neues Video zeigt dir, wie Cookies dein Online-Verhalten verfolgen und wie du dich davor schützen kannst! #Cookies #PersonalisierteWerbung #Datenschutz #DSGVO“

Beitrag 3: Aufklärungsflyer

- Bild: Der Flyer über Cookies und Datenschutz.
- Text (Post-Beschreibung): „📄 Lade unseren Flyer herunter und erfahre, wie du deine Daten vor unerwünschtem Tracking schützen kannst! #Flyer #Datenschutz #DSGVO #Cookies“

Zusätzliche Posts:

Post-Idee 1: Quiz zur Nutzung von Cookies

- Bild: Ein interaktives Bild mit der Quiz-Frage: „Weißt du, wie Cookies dein Online-Verhalten verfolgen?“ mit Antwortmöglichkeiten wie: „Ja, aber mir egal!“ oder „Nein, das ist mir neu!“.
- Text: „Teste dein Wissen! Erfahre, wie Social Media-Plattformen Cookies nutzen, um dich zu verfolgen. Nimm an unserem Quiz teil und finde es heraus! #Cookies #Datenschutz #Quiz #DSGVO“

Post-Idee 2: Fakten über Cookies und personalisierte Werbung

- Bild: Eine Infografik mit Fakten zu Cookies und personalisierter Werbung, z.B.: „Cookies speichern deine Online-Aktivitäten, um personalisierte Werbung zu schalten. Weißt du, wie du das kontrollieren kannst?“.
- Text: „Schon gewusst? Websites und Social Media nutzen Cookies, um dein Verhalten zu verfolgen und Werbung zu schalten. Erfahre, wie du deine Daten schützen kannst! #Cookies #Datensicherheit #PersonalisierteWerbung #DSGVO“

Story-Idee: Umfrage zu Cookies und Datenschutz

- Frage: „Weißt du, wie Cookies deine Online-Aktivitäten verfolgen?“
- Optionen: „Ja, ich passe auf!“ / „Nein, keine Ahnung!“
- Ergebnis: Bei „Nein“ könnte ein Swipe-up-Link zu einem erklärenden Video oder einem Infopost geleitet werden.

Post-Idee 3: Tutorial zum Datenschutz bei Cookies

- Bild: Ein Bild eines Cookie-Symbols mit einem Datenschutz-Symbol daneben.
- Text: „Cookies können dein Verhalten im Netz verfolgen – auch für Werbezwecke. Erfahre in unserem Tutorial, wie du die Datenschutzeinstellungen deines Browsers anpassen kannst, um dich besser zu schützen. #Cookies #Datenschutz #DSGVO #SicherImNetz“

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

DEEPPFAKES

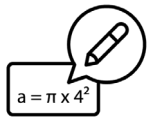
AI generierte Inhalte, wie Videos, Audios und Deepfakes werden immer häufiger und einfacher zu erstellen. Dies lässt einen unglaublichen Raum an Manipulation zu. Liegen genügend Daten (Bilddaten, Audiodaten, ...) über eine Person vor, dann kann man problemlos ein Deepfake dieser Person erstellen. Dazu wird KI mit Hilfe von Big Data trainiert. Dies birgt die Gefahr von Desinformationskampagnen, Identitätsdiebstahl und Privatsphäreverletzungen. Fake News, politische Manipulation und Rufschädigung sind nur wenige der potenziellen Risiken.

PODCAST

Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



DeepFakes - Real oder nicht?

AI-generierte Inhalte, wie Videos, Audios und DeepFakes, stellen eine der neuesten technologischen Entwicklungen dar, die durch Big Data und Künstliche Intelligenz (KI) ermöglicht werden. Diese Technologien erlauben es, täuschend echte, aber vollkommen künstliche Videos und Audioaufnahmen zu erstellen. So kann man beispielsweise das Gesicht einer Person in einem Video manipulieren oder die Stimme einer anderen Person so nachahmen, dass es scheint, als hätte diese Person etwas gesagt, was sie nie gesagt hat.

Der Schlüssel zu dieser Technologie liegt in Big Data: Die KI wird mit riesigen Datenmengen trainiert, um menschliche Mimik, Stimme und Gesten nachzubilden. Plattformen wie YouTube, TikTok und andere soziale Medien können durch diese Entwicklungen stark beeinflusst werden, da gefälschte Inhalte immer realistischer und schwieriger zu erkennen werden.

Während AI-generierte Inhalte und DeepFakes in der Film- und Unterhaltungsindustrie nützliche Werkzeuge sein können, gibt es auch erhebliche Bedenken bezüglich Desinformation, Identitätsdiebstahl und Privatsphärenverletzungen. Fake News, politische Manipulation, Rufschädigung und Betrug sind nur einige der potenziellen Risiken, die durch diese Technologien entstehen.

Die **Datenschutz-Grundverordnung (DSGVO)** schützt personenbezogene Daten und bietet Betroffenen das Recht auf Löschung oder Einsicht in ihre Daten. Doch die Rechtslage in Bezug auf die Erstellung und Verbreitung von AI-generierten Inhalten bleibt eine Herausforderung.

Beispiele für DeepFake/AI-generated:



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind AI-generierte Videos und Audios, und wie werden sie erstellt?
- Welche Regeln der DSGVO/anderer Gesetze schützen dich vor dem Missbrauch von AI-generierten Inhalten und DeepFakes?
- Wie beeinflussen AI-generierte Inhalte und DeepFakes die Privatsphäre und das Persönlichkeitsrecht?
- Welche Risiken können durch DeepFakes oder KI-generierte Inhalte entstehen? Welche Chancen bieten sie?
- Wie kannst du sicherstellen, dass keine AI-generierten Inhalte von dir erstellt werden?

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



QR 2: DSGVO Art. 17
"Recht auf
Vergessenwerden"



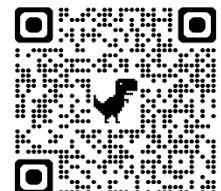
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am
eigenen Bild

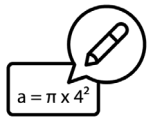


QR 2: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



1. Podcast-Interviewer-Leitfaden (5-Minuten Podcast)

Thema: „AI-generierte Inhalte und DeepFakes: Manipulation im digitalen Zeitalter“

1. Einleitung:

„Willkommen zu unserem Podcast! Heute sprechen wir über AI-generierte Videos, Audios und DeepFakes und wie Big Data diese Technologien ermöglicht. Wir beleuchten, wie diese Inhalte erstellt werden, und welche Risiken sie für unsere Gesellschaft und Privatsphäre darstellen.“

2. Frage 1:

„Was genau sind AI-generierte Videos und Audios, und wie werden sie erstellt?“

(Ziel: Einführung in die Technologie, die hinter AI-generierten Inhalten steht, und welche Rolle Big Data dabei spielt.)

3. Frage 2:

„Welche Gefahren gehen von AI-generierten Inhalten und DeepFakes aus, besonders im Zusammenhang mit Fake News und Privatsphäre?“

(Ziel: Diskussion der Auswirkungen von gefälschten Videos und Audios auf das soziale und politische Umfeld sowie auf die Privatsphäre von Einzelpersonen.)

4. Frage 3:

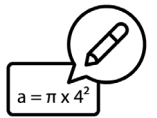
„Welche Rolle spielt die DSGVO beim Schutz vor AI-generierten Inhalten?“

(Ziel: Erklärung der gesetzlichen Bestimmungen, insbesondere des Rechts am eigenen Bild und des Rechts auf Vergessenwerden.)

5. Frage 4:

„Wie können sich Betroffene schützen, wenn sie durch AI-generierte Videos oder Audios in ihrer Privatsphäre verletzt werden?“

(Ziel: Praktische Tipps zum Schutz der eigenen Daten und der eigenen Identität.)



DeepFakes - Real oder nicht?

AI-generierte Inhalte, wie Videos, Audios und DeepFakes, stellen eine der neuesten technologischen Entwicklungen dar, die durch Big Data und Künstliche Intelligenz (KI) ermöglicht werden. Diese Technologien erlauben es, täuschend echte, aber vollkommen künstliche Videos und Audioaufnahmen zu erstellen. So kann man beispielsweise das Gesicht einer Person in einem Video manipulieren oder die Stimme einer anderen Person so nachahmen, dass es scheint, als hätte diese Person etwas gesagt, was sie nie gesagt hat.

Der Schlüssel zu dieser Technologie liegt in Big Data: Die KI wird mit riesigen Datenmengen trainiert, um menschliche Mimik, Stimme und Gesten nachzubilden. Plattformen wie YouTube, TikTok und andere soziale Medien können durch diese Entwicklungen stark beeinflusst werden, da gefälschte Inhalte immer realistischer und schwieriger zu erkennen werden.

Während AI-generierte Inhalte und DeepFakes in der Film- und Unterhaltungsindustrie nützliche Werkzeuge sein können, gibt es auch erhebliche Bedenken bezüglich Desinformation, Identitätsdiebstahl und Privatsphärenverletzungen. Fake News, politische Manipulation, Rufschädigung und Betrug sind nur einige der potenziellen Risiken, die durch diese Technologien entstehen.

Die **Datenschutz-Grundverordnung (DSGVO)** schützt personenbezogene Daten und bietet Betroffenen das Recht auf Löschung oder Einsicht in ihre Daten. Doch die Rechtslage in Bezug auf die Erstellung und Verbreitung von AI-generierten Inhalten bleibt eine Herausforderung.

Beispiele für DeepFake/AI-generated:



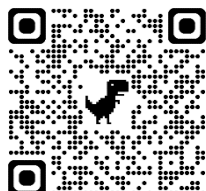
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind AI-generierte Videos und Audios, und wie werden sie erstellt?
- Welche Regeln der DSGVO/anderer Gesetze schützen dich vor dem Missbrauch von AI-generierten Inhalten und DeepFakes?
- Wie beeinflussen AI-generierte Inhalte und DeepFakes die Privatsphäre und das Persönlichkeitsrecht?
- Welche Risiken können durch DeepFakes oder KI-generierte Inhalte entstehen? Welche Chancen bieten sie?
- Wie kannst du sicherstellen, dass keine AI-generierten Inhalte von dir erstellt werden?

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, das alles Relevante dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze movier/Clips zum Erstellen und Bearbeiten der Inhalte.



QR 4: DSGVO Art. 17
"Recht auf Vergessenwerden"



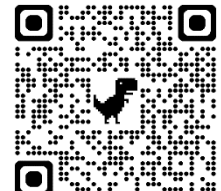
QR 2: DSGVO Art. 9
Verarbeitung personenbezogener Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am eigenen Bild



QR 4: DSGVO Art. 6
"Rechtmäßigkeit der Verarbeitung"

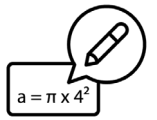


Weitere Quellen:

- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



DEEPPFAKES DURCH BIGDATA



Szenenbeschreibung für ein 2-Minuten-Video

Titel: „AI-generierte Videos und Audios: Was ist echt und was ist manipuliert?“

Ort: Ein belebter Platz in der Stadt. Person A schaut sich auf ihrem Smartphone ein Video an, das scheinbar eine berühmte Persönlichkeit zeigt. Neben ihr steht Person B und beobachtet die Reaktion.

Person A (überrascht): „Das gibt’s doch nicht! Ich hätte nie gedacht, dass dieser Schauspieler so etwas sagt.“

Person B (wissend): „Bist du sicher, dass das echt ist? Es könnte ein AI-generiertes Video sein.“

Person A (verwirrt): „Was meinst du?“

Person B (erklärend): „AI-generierte Videos sind von Künstlicher Intelligenz erstellt. Sie können das Gesicht und die Stimme einer Person perfekt nachahmen. Es sieht echt aus, aber es ist komplett gefälscht.“

Person A (besorgt): „Und woher soll ich wissen, dass das ein Fake ist?“

Person B (ruhig): „Es gibt einige Hinweise, wie etwa unnatürliche Bewegungen oder merkwürdige Verzögerungen in der Sprache. Aber die Fälschungen werden immer besser.“

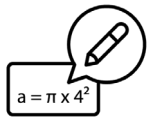
Person A (nachdenklich): „Und wenn jemand so ein Fake von mir macht?“

Person B (ernst): „Du hast das Recht, solche Inhalte löschen zu lassen, aber das ist nicht immer einfach.“

Schlusszene:

Text auf dem Bildschirm: „Schütze deine digitale Identität. AI-generierte Inhalte und DeepFakes sind keine Spielerei. #DSGVO #DeepFakes #AI-Content #BigData“

Voiceover: „Erfahre, wie du dich vor digitalen Fälschungen schützen kannst. Deine Daten und deine Identität sind wertvoll.“



DeepFakes - Real oder nicht?

AI-generierte Inhalte, wie Videos, Audios und DeepFakes, stellen eine der neuesten technologischen Entwicklungen dar, die durch Big Data und Künstliche Intelligenz (KI) ermöglicht werden. Diese Technologien erlauben es, täuschend echte, aber vollkommen künstliche Videos und Audioaufnahmen zu erstellen. So kann man beispielsweise das Gesicht einer Person in einem Video manipulieren oder die Stimme einer anderen Person so nachahmen, dass es scheint, als hätte diese Person etwas gesagt, was sie nie gesagt hat.

Der Schlüssel zu dieser Technologie liegt in Big Data: Die KI wird mit riesigen Datenmengen trainiert, um menschliche Mimik, Stimme und Gesten nachzubilden. Plattformen wie YouTube, TikTok und andere soziale Medien können durch diese Entwicklungen stark beeinflusst werden, da gefälschte Inhalte immer realistischer und schwieriger zu erkennen werden.

Während AI-generierte Inhalte und DeepFakes in der Film- und Unterhaltungsindustrie nützliche Werkzeuge sein können, gibt es auch erhebliche Bedenken bezüglich Desinformation, Identitätsdiebstahl und Privatsphärenverletzungen. Fake News, politische Manipulation, Rufschädigung und Betrug sind nur einige der potenziellen Risiken, die durch diese Technologien entstehen.

Die **Datenschutz-Grundverordnung (DSGVO)** schützt personenbezogene Daten und bietet Betroffenen das Recht auf Löschung oder Einsicht in ihre Daten. Doch die Rechtslage in Bezug auf die Erstellung und Verbreitung von AI-generierten Inhalten bleibt eine Herausforderung.

Beispiele für DeepFake/AI-generated:



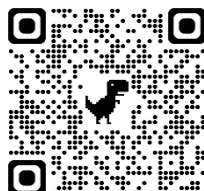
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind AI-generierte Videos und Audios, und wie werden sie erstellt?
- Welche Regeln der DSGVO/anderer Gesetze schützen dich vor dem Missbrauch von AI-generierten Inhalten und DeepFakes?
- Wie beeinflussen AI-generierte Inhalte und DeepFakes die Privatsphäre und das Persönlichkeitsrecht?
- Welche Risiken können durch DeepFakes oder KI-generierte Inhalte entstehen? Welche Chancen bieten sie?
- Wie kannst du sicherstellen, dass keine AI-generierten Inhalte von dir erstellt werden?

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



QR 6: DSGVO Art. 17
"Recht auf
Vergessenwerden"



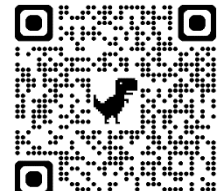
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am
eigenen Bild



QR 6: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

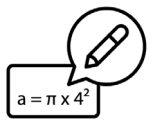


Weitere Quellen:

- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



DEEPPFAKES DURCH BIGDATA



Flyer-Inhalt (KI-generiert):

1. Überschrift:

- **Position:** Oben, zentriert.
- **Text:** „Schon gewusst?“ in großer, fetter Schrift.
- **Schriftart:** Moderne, klare Schriftart (z.B. Arial oder Helvetica).
- **Farbe:** Blau, um Aufmerksamkeit zu erregen.

2. Einleitender Text:

- **Position:** Direkt unter der Überschrift.
- **Text:** Eine kurze Erklärung, wie AI-generierte Inhalte durch Big Data und KI erstellt werden und welche Risiken sie für die Privatsphäre darstellen.
- **Schriftart:** Kleinere, gut lesbare Schrift.
- **Farbe:** Schwarz oder dunkles Grau.

3. Fakten und Tipps:

- **Position:** In der Mitte, als Liste angeordnet.
- **Text:** 3–4 Tipps, wie z.B. „Überprüfe deine Datenschutzeinstellungen regelmäßig“, „Lerne, wie du AI-generierte Inhalte erkennst“, „Nutze dein Recht, DeepFakes gemäß DSGVO entfernen zu lassen“.
- **Schriftart:** Leicht hervorgehoben, fett oder kursiv, damit die Tipps ins Auge fallen.
- **Farbe:** Schwarz für den Text, Blau für Aufzählungspunkte oder Nummern.

4. Grafik/Symbol:

- **Position:** Unten rechts.
- **Bild:** Ein Symbol eines geteilten Gesichts oder eines Datenschutzschildes.
- **Größe:** Dezent und klein, um den Text zu unterstreichen.

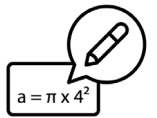
5. Abschlusssatz:

- **Position:** Unten links, neben der Grafik.
- **Text:** „Bleib informiert und schütze deine digitale Identität. #DSGVO #DeepFakes #AIContent.“
- **Schriftart:** Klein, aber gut lesbar.
- **Farbe:** Blau oder Grau, um sich harmonisch in das Design einzufügen.

Gestaltungstipps:

- Nutze weißen Raum, um den Flyer nicht zu überladen.
- Symmetrische Anordnung hilft, das Design sauber und professionell wirken zu lassen.





DeepFakes - Real oder nicht?

AI-generierte Inhalte, wie Videos, Audios und DeepFakes, stellen eine der neuesten technologischen Entwicklungen dar, die durch Big Data und Künstliche Intelligenz (KI) ermöglicht werden. Diese Technologien erlauben es, täuschend echte, aber vollkommen künstliche Videos und Audioaufnahmen zu erstellen. So kann man beispielsweise das Gesicht einer Person in einem Video manipulieren oder die Stimme einer anderen Person so nachahmen, dass es scheint, als hätte diese Person etwas gesagt, was sie nie gesagt hat.

Der Schlüssel zu dieser Technologie liegt in Big Data: Die KI wird mit riesigen Datenmengen trainiert, um menschliche Mimik, Stimme und Gesten nachzubilden. Plattformen wie YouTube, TikTok und andere soziale Medien können durch diese Entwicklungen stark beeinflusst werden, da gefälschte Inhalte immer realistischer und schwieriger zu erkennen werden.

Während AI-generierte Inhalte und DeepFakes in der Film- und Unterhaltungsindustrie nützliche Werkzeuge sein können, gibt es auch erhebliche Bedenken bezüglich Desinformation, Identitätsdiebstahl und Privatsphärenverletzungen. Fake News, politische Manipulation, Rufschädigung und Betrug sind nur einige der potenziellen Risiken, die durch diese Technologien entstehen.

Die **Datenschutz-Grundverordnung (DSGVO)** schützt personenbezogene Daten und bietet Betroffenen das Recht auf Löschung oder Einsicht in ihre Daten. Doch die Rechtslage in Bezug auf die Erstellung und Verbreitung von AI-generierten Inhalten bleibt eine Herausforderung.

Beispiele für DeepFake/AI-generated:



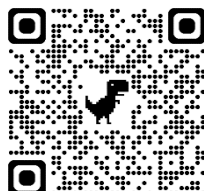
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind AI-generierte Videos und Audios, und wie werden sie erstellt?
- Welche Regeln der DSGVO/anderer Gesetze schützen dich vor dem Missbrauch von AI-generierten Inhalten und DeepFakes?
- Wie beeinflussen AI-generierte Inhalte und DeepFakes die Privatsphäre und das Persönlichkeitsrecht?
- Welche Risiken können durch DeepFakes oder KI-generierte Inhalte entstehen? Welche Chancen bieten sie?
- Wie kannst du sicherstellen, dass keine AI-generierten Inhalte von dir erstellt werden?

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



QR 8: DSGVO Art. 17
"Recht auf
Vergessenwerden"



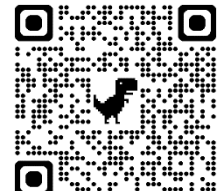
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: Recht am
eigenen Bild



QR 8: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

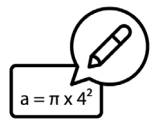


Weitere Quellen:

- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



DEEPPAKES DURCH BIGDATA



Beiträge der Kampagne:

Beitrag 1: Podcast-Ankündigung

- Bild/Video: Ein animiertes Bild mit dem Titel „AI-generierte Inhalte: Was du wissen musst“ und einem Play-Button.
- Text (Post-Beschreibung): „🎧 Weißt du, wie AI und Big Data genutzt werden, um DeepFakes und gefälschte Inhalte zu erstellen? Erfahre in unserem neuen Podcast, wie du dich davor schützen kannst.
➡ Hör jetzt rein! #DeepFakes #AIContent #BigData #DSGVO #Privatsphäre“

Beitrag 2: 2-Minuten-Video „Echte oder gefälschte Inhalte?“

- Bild/Video: Ein 2-minütiges Video, das eine Unterhaltung über die Risiken von AI-generierten Videos und Audios zeigt.
- Text (Post-Beschreibung): „👁️ Kannst du echte Inhalte von AI-generierten Fälschungen unterscheiden? In unserem neuen Video erfährst du, wie DeepFakes funktionieren und wie du dich schützen kannst! #AIContent #DeepFakes #BigData #Datenschutz #DSGVO“

Beitrag 3: Aufklärungsflyer

- Bild: Der Flyer über AI-generierte Inhalte und Datenschutz (siehe Beispiel-Flyer oben).
- Text (Post-Beschreibung): „📄 Lade unseren Flyer herunter und erfahre, wie du deine digitale Identität vor DeepFakes und AI-generierten Inhalten schützen kannst! #Flyer #DeepFakes #Datenschutz #AIContent #BigData“

Zusätzliche Post-Ideen:

Post-Idee 1: Quiz zur Erkennung von DeepFakes

- Bild: Ein interaktives Bild mit der Quiz-Frage: „Kannst du den Unterschied zwischen echtem und gefälschtem Video erkennen?“ mit Antwortmöglichkeiten wie: „Ja, ich bin mir sicher!“ oder „Nein, das ist schwierig!“.
- Text: „Teste dein Wissen! Weißt du, wie man DeepFakes und AI-generierte Inhalte erkennt? Nimm an unserem Quiz teil und finde es heraus! #DeepFakes #AIContent #Quiz #Datenschutz #DSGVO“

Post-Idee 2: Fakten über AI-generierte Inhalte und Datenschutz

- Bild: Eine Infografik mit Fakten zu DeepFakes und AI-generierten Inhalten, z.B.: „Wusstest du, dass deine Stimme und dein Gesicht für gefälschte Videos verwendet werden können? Lerne, wie du deine Rechte schützt!“.
- Text: „Schon gewusst? AI-generierte Inhalte können leicht missbraucht werden. Erfahre, wie du deine Privatsphäre schützen kannst! #DeepFakes #Datensicherheit #AIContent #DSGVO“

Story-Idee: Umfrage zu AI-Inhalten und Datenschutz

- Frage: „Weißt du, wie AI-generierte Inhalte erstellt werden? Glaubst du, deine Daten sind sicher?“
- Optionen: „Ja, ich weiß es!“ / „Nein, keine Ahnung!“
- Ergebnis: Bei „Nein“ könnte ein Swipe-up-Link zu einem erklärenden Video oder einem Infopost geleitet werden.

Post-Idee 3: Tutorial zum Schutz vor AI-generierten Inhalten

- Bild: Ein Bild von einer digitalen Figur oder einem Symbol für Datenschutz, das auf die Manipulation durch AI hinweist.
- Text:
„Deine digitale Identität ist wertvoll – auch für diejenigen, die AI nutzen. Erfahre in unserem Tutorial, wie du deine Daten schützt und AI-generierte Inhalte erkennst!
#AIContent #Datenschutz #DSGVO #SicherImNetz“

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

SPRACHASSISTENTEN

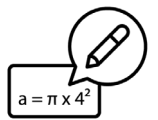
KI gestützte Sprachassistenten, wie in Chatbots oder persönlichen Assistenten (Alexa, Siri, Google Assistant, ...) sind mittlerweile tägliche Begleiter. Die Sprachmodelle dieser Assistenten verarbeiten Unmengen an Daten, um zu trainieren und besser zu werden. Dabei rufen sie Daten aus Smart-Home-Geräten oder der Smartphones ab. Das führt zum Beispiel dazu, dass Sprachassistenten über die Mikrofonaufnahme theoretisch jederzeit zuhören kann. Wie werden diese private Daten kommerzialisiert oder missbraucht?

PODCAST

Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



Warum werden Siri, Alexa und Google-Assistant immer besser?

KI-gestützte Chatbots und persönliche Assistenten wie Siri, Alexa und Google Assistant sind mittlerweile alltägliche Begleiter. Diese Technologien nutzen Natural Language Processing (NLP) und Big Data, um gesprochene Sprache zu verstehen und darauf zu reagieren. Sie ermöglichen es, menschliche Sprache in maschinell verarbeitbare Befehle umzuwandeln, was wiederum die Erledigung von Aufgaben wie das Abspielen von Musik, das Steuern von Smart-Home-Geräten oder das Abrufen von Informationen erlaubt. Sprachassistenten greifen auf riesige Datenmengen zurück, um Antworten zu generieren und ihre Leistung kontinuierlich zu verbessern. Dabei spielen maschinelles Lernen und Cloud-Speicherung eine zentrale Rolle, da die Anfragen der Nutzer in der Cloud verarbeitet und gespeichert werden, was den Assistenten ermöglicht, sich an die Präferenzen der Nutzer anzupassen und ihre Dienste zu optimieren.

Trotz der vielen Vorteile, die Sprachassistenten bieten, stehen sie unter ständiger Kritik, vor allem in Bezug auf den Datenschutz. Da viele dieser Systeme dauerhaft aktiviert sind, besteht die Gefahr, dass sie Gespräche mithören und private Informationen aufzeichnen, ohne dass die Nutzer es bewusst wahrnehmen. Die gesammelten Daten werden oft für kommerzielle Zwecke genutzt, wie etwa die Schaltung personalisierter Werbung, was zu einem erheblichen Vertrauensverlust führen kann. Die Nutzung von Big Data ist dabei der Schlüssel zu ihrer Leistungsfähigkeit: Je mehr Daten diese Assistenten sammeln, desto besser können sie die Bedürfnisse der Nutzer voraussagen und ihre Antworten personalisieren. Gleichzeitig wirft dieser ständige Datenfluss ethische Fragen auf, da nicht immer klar ist, wer Zugriff auf diese Daten hat und wie sie verwendet werden.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren KI-gestützte Chatbots und Sprachassistenten?
- Wo werden KI-gestützte Chatbots oder Sprachassistenten überall eingesetzt?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch KI-gestützte Assistenten?
- Welche Risiken bestehen durch die Nutzung von Sprachassistenten für deine Privatsphäre?
- In welchen alltäglichen Kontexten kann die Technik problematisch sein?
- Wie kannst du deine Daten schützen, wenn du KI-Assistenten nutzt?

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



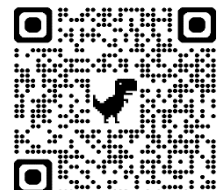
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht au
Widerspruch

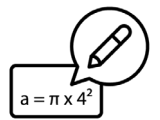


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

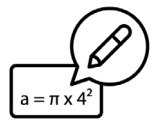
- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



1. Podcast-Interviewer-Leitfaden (5-Minuten Podcast)

Thema: „Sprachassistenten und Chatbots: Helfer oder Spione?“

1. Einleitung:
„Willkommen zu unserem Podcast! Heute sprechen wir über KI-gestützte Sprachassistenten und Chatbots und wie sie unser Leben erleichtern – aber auch, welche Risiken sie für unsere Privatsphäre mit sich bringen.“
2. Frage 1:
„Wie funktionieren Sprachassistenten wie Siri, Alexa und Google Assistant?“
(Ziel: Einführung in die Technologie hinter den Assistenten und wie sie natürliche Sprache verarbeiten.)
3. Frage 2:
„Welche Risiken bestehen bei der Nutzung dieser Technologien, insbesondere in Bezug auf die Privatsphäre?“
(Ziel: Diskutiere die Gefahren von Datensammlungen und unerwünschtem Mithören durch die Assistenten.)
4. Frage 3:
„Welche Rolle spielt die DSGVO beim Schutz vor dem Missbrauch von KI-gestützten Assistenten?“
(Ziel: Erkläre, wie die DSGVO dazu beiträgt, dass Nutzer ihre Rechte auf Einsicht und Löschung ihrer Daten geltend machen können.)
5. Frage 4:
„Wie können sich Nutzer vor unerwünschtem Datenmissbrauch schützen?“
(Ziel: Biete praktische Tipps, wie Nutzer ihre Sprachassistenten sicher nutzen können.)



Warum werden Siri, Alexa und Google-Assistant immer besser?

KI-gestützte Chatbots und persönliche Assistenten wie Siri, Alexa und Google Assistant sind mittlerweile alltägliche Begleiter. Diese Technologien nutzen Natural Language Processing (NLP) und Big Data, um gesprochene Sprache zu verstehen und darauf zu reagieren. Sie ermöglichen es, menschliche Sprache in maschinell verarbeitbare Befehle umzuwandeln, was wiederum die Erledigung von Aufgaben wie das Abspielen von Musik, das Steuern von Smart-Home-Geräten oder das Abrufen von Informationen erlaubt. Sprachassistenten greifen auf riesige Datenmengen zurück, um Antworten zu generieren und ihre Leistung kontinuierlich zu verbessern. Dabei spielen maschinelles Lernen und Cloud-Speicherung eine zentrale Rolle, da die Anfragen der Nutzer in der Cloud verarbeitet und gespeichert werden, was den Assistenten ermöglicht, sich an die Präferenzen der Nutzer anzupassen und ihre Dienste zu optimieren.

Trotz der vielen Vorteile, die Sprachassistenten bieten, stehen sie unter ständiger Kritik, vor allem in Bezug auf den Datenschutz. Da viele dieser Systeme dauerhaft aktiviert sind, besteht die Gefahr, dass sie Gespräche mithören und private Informationen aufzeichnen, ohne dass die Nutzer es bewusst wahrnehmen. Die gesammelten Daten werden oft für kommerzielle Zwecke genutzt, wie etwa die Schaltung personalisierter Werbung, was zu einem erheblichen Vertrauensverlust führen kann. Die Nutzung von Big Data ist dabei der Schlüssel zu ihrer Leistungsfähigkeit: Je mehr Daten diese Assistenten sammeln, desto besser können sie die Bedürfnisse der Nutzer voraussagen und ihre Antworten personalisieren. Gleichzeitig wirft dieser ständige Datenfluss ethische Fragen auf, da nicht immer klar ist, wer Zugriff auf diese Daten hat und wie sie verwendet werden.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren KI-gestützte Chatbots und Sprachassistenten?
- Wo werden KI-gestützte Chatbots oder Sprachassistenten überall eingesetzt?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch KI-gestützte Assistenten?
- Welche Risiken bestehen durch die Nutzung von Sprachassistenten für deine Privatsphäre?
- In welchen alltäglichen Kontexten kann die Technik problematisch sein?
- Wie kannst du deine Daten schützen, wenn du KI-Assistenten nutzt?

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, das alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze iMovie/Clips zum Erstellen und Bearbeiten der Inhalte.



QR 2: DSGVO Art. 17
"Recht auf
Vergessenwerden"



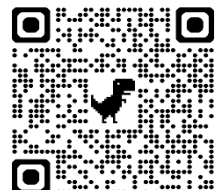
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht au
Widerspruch

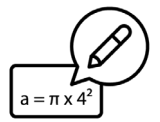


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



Szenenbeschreibung für ein 2-Minuten-Video

Titel: „Was Siri, Alexa und Google Assistant wirklich über dich wissen“

Ort: Wohnzimmer. Person A spricht mit ihrem Sprachassistenten, während Person B aufmerksam zuhört.

Person A (sprechen mit dem Assistenten): „Hey Siri, wie wird das Wetter heute?“

Siri: „Heute wird es sonnig bei 24 Grad.“

Person B (neugierig): „Weißt du, dass Siri mehr über dich weiß, als du denkst?“

Person A (verwirrt): „Was meinst du?“

Person B (erklärend): „Siri und andere Sprachassistenten hören immer zu, auch wenn du es nicht aktivierst. Sie sammeln deine Daten – nicht nur, um dir das Wetter zu sagen, sondern auch für andere Zwecke.“

Person A (besorgt): „Wirklich? Welche Daten sammeln sie denn?“

Person B (ernst): „Alles, was du sagst, wo du bist und was du tust. Diese Informationen werden genutzt, um dir personalisierte Werbung zu zeigen oder sogar deine Vorlieben vorherzusagen.“

Person A (entschlossen): „Das klingt beunruhigend. Ich werde nachsehen, welche Daten Siri von mir gespeichert hat.“

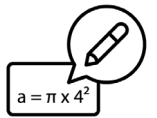
Schlusszene:

Text auf dem Bildschirm: „Schütze deine Privatsphäre. Überprüfe, welche Daten dein Assistent über dich sammelt. #DSGVO #KI #Sprachassistenten“

Voiceover: „Erfahre, wie du deine Daten schützen kannst.“



CHATBOTS UND SPRACHASSISTENTEN



Warum werden Siri, Alexa und Google-Assistant immer besser?

KI-gestützte Chatbots und persönliche Assistenten wie Siri, Alexa und Google Assistant sind mittlerweile alltägliche Begleiter. Diese Technologien nutzen Natural Language Processing (NLP) und Big Data, um gesprochene Sprache zu verstehen und darauf zu reagieren. Sie ermöglichen es, menschliche Sprache in maschinell verarbeitbare Befehle umzuwandeln, was wiederum die Erledigung von Aufgaben wie das Abspielen von Musik, das Steuern von Smart-Home-Geräten oder das Abrufen von Informationen erlaubt. Sprachassistenten greifen auf riesige Datenmengen zurück, um Antworten zu generieren und ihre Leistung kontinuierlich zu verbessern. Dabei spielen maschinelles Lernen und Cloud-Speicherung eine zentrale Rolle, da die Anfragen der Nutzer in der Cloud verarbeitet und gespeichert werden, was den Assistenten ermöglicht, sich an die Präferenzen der Nutzer anzupassen und ihre Dienste zu optimieren.

Trotz der vielen Vorteile, die Sprachassistenten bieten, stehen sie unter ständiger Kritik, vor allem in Bezug auf den Datenschutz. Da viele dieser Systeme dauerhaft aktiviert sind, besteht die Gefahr, dass sie Gespräche mithören und private Informationen aufzeichnen, ohne dass die Nutzer es bewusst wahrnehmen. Die gesammelten Daten werden oft für kommerzielle Zwecke genutzt, wie etwa die Schaltung personalisierter Werbung, was zu einem erheblichen Vertrauensverlust führen kann. Die Nutzung von Big Data ist dabei der Schlüssel zu ihrer Leistungsfähigkeit: Je mehr Daten diese Assistenten sammeln, desto besser können sie die Bedürfnisse der Nutzer voraussagen und ihre Antworten personalisieren. Gleichzeitig wirft dieser ständige Datenfluss ethische Fragen auf, da nicht immer klar ist, wer Zugriff auf diese Daten hat und wie sie verwendet werden.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren KI-gestützte Chatbots und Sprachassistenten?
- Wo werden KI-gestützte Chatbots oder Sprachassistenten überall eingesetzt?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch KI-gestützte Assistenten?
- Welche Risiken bestehen durch die Nutzung von Sprachassistenten für deine Privatsphäre?
- In welchen alltäglichen Kontexten kann die Technik problematisch sein?
- Wie kannst du deine Daten schützen, wenn du KI-Assistenten nutzt?

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



QR 3: DSGVO Art. 17
"Recht auf
Vergessenwerden"



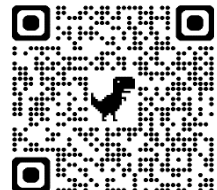
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht au
Widerspruch

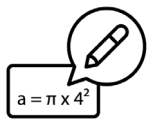


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



Flyer-Inhalt: „Schon gewusst?“ – KI-gestützte Chatbots und persönliche Assistenten (KI generiert)

1. Überschrift:

- **Position:** Oben, zentriert.
- **Text:** „Schon gewusst?“ in großer, fatter Schrift.
- **Schriftart:** Moderne, klare Schriftart (z.B. Arial oder Helvetica).
- **Farbe:** Blau, um Aufmerksamkeit zu erregen.

2. Einleitender Text:

- **Position:** Direkt unter der Überschrift.
- **Text:** Eine kurze Erklärung, wie Chatbots und persönliche Assistenten wie Siri, Alexa und Google Assistant mit Hilfe von KI und Big Data arbeiten und welche Datenschutzrisiken bestehen.
- **Schriftart:** Kleinere, gut lesbare Schrift.
- **Farbe:** Schwarz oder dunkles Grau.

3. Fakten und Tipps:

- **Position:** In der Mitte, als Liste angeordnet.
- **Text:** 3–4 Tipps, wie z.B. „Überprüfe deine Datenschutzeinstellungen regelmäßig“, „Deaktiviere Mikrofone, wenn sie nicht gebraucht werden“, „Nutze deine DSGVO-Rechte zur Löschung von Daten“.
- **Schriftart:** Leicht hervorgehoben (z.B. fett oder kursiv), damit die Tipps ins Auge fallen.
- **Farbe:** Schwarz für den Text, Blau für Aufzählungspunkte oder Nummern, um die Liste hervorzuheben.

4. Grafik/Symbol:

- **Position:** Unten rechts.
- **Bild:** Ein Symbol, das eine Sprechblase und ein Datenschutzschild kombiniert.
- **Größe:** Dezent und klein, um den Text zu unterstreichen.

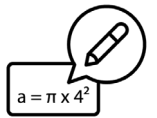
5. Abschlusssatz:

- **Position:** Unten links, neben der Grafik.
- **Text:** „Bleib informiert und schütze deine Privatsphäre. #DSGVO #Sprachassistenten #BigData.“
- **Schriftart:** Klein, aber gut lesbar.
- **Farbe:** Blau oder Grau, um sich harmonisch in das Design einzufügen.



Gestaltungstipps:

- Nutze weißen Raum, um den Flyer nicht zu überladen.
- Symmetrische Anordnung hilft, das Design sauber und professionell wirken zu lassen



Warum werden Siri, Alexa und Google-Assistant immer besser?

KI-gestützte Chatbots und persönliche Assistenten wie Siri, Alexa und Google Assistant sind mittlerweile alltägliche Begleiter. Diese Technologien nutzen Natural Language Processing (NLP) und Big Data, um gesprochene Sprache zu verstehen und darauf zu reagieren. Sie ermöglichen es, menschliche Sprache in maschinell verarbeitbare Befehle umzuwandeln, was wiederum die Erledigung von Aufgaben wie das Abspielen von Musik, das Steuern von Smart-Home-Geräten oder das Abrufen von Informationen erlaubt. Sprachassistenten greifen auf riesige Datenmengen zurück, um Antworten zu generieren und ihre Leistung kontinuierlich zu verbessern. Dabei spielen maschinelles Lernen und Cloud-Speicherung eine zentrale Rolle, da die Anfragen der Nutzer in der Cloud verarbeitet und gespeichert werden, was den Assistenten ermöglicht, sich an die Präferenzen der Nutzer anzupassen und ihre Dienste zu optimieren.

Trotz der vielen Vorteile, die Sprachassistenten bieten, stehen sie unter ständiger Kritik, vor allem in Bezug auf den Datenschutz. Da viele dieser Systeme dauerhaft aktiviert sind, besteht die Gefahr, dass sie Gespräche mithören und private Informationen aufzeichnen, ohne dass die Nutzer es bewusst wahrnehmen. Die gesammelten Daten werden oft für kommerzielle Zwecke genutzt, wie etwa die Schaltung personalisierter Werbung, was zu einem erheblichen Vertrauensverlust führen kann. Die Nutzung von Big Data ist dabei der Schlüssel zu ihrer Leistungsfähigkeit: Je mehr Daten diese Assistenten sammeln, desto besser können sie die Bedürfnisse der Nutzer voraussagen und ihre Antworten personalisieren. Gleichzeitig wirft dieser ständige Datenfluss ethische Fragen auf, da nicht immer klar ist, wer Zugriff auf diese Daten hat und wie sie verwendet werden.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren KI-gestützte Chatbots und Sprachassistenten?
- Wo werden KI-gestützte Chatbots oder Sprachassistenten überall eingesetzt?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch KI-gestützte Assistenten?
- Welche Risiken bestehen durch die Nutzung von Sprachassistenten für deine Privatsphäre?
- In welchen alltäglichen Kontexten kann die Technik problematisch sein?
- Wie kannst du deine Daten schützen, wenn du KI-Assistenten nutzt?

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



QR 4: DSGVO Art. 17
"Recht auf
Vergessenwerden"



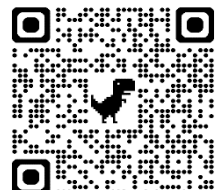
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3:
Urheberrechtsgesetz



QR 4: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch

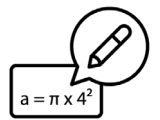


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- BSI.bund.de:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- AI-Act der EU:
https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
- Netzpolitik zu Manipulation im Netz:
<https://netzpolitik.org/2021/dark-patterns-eu-abgeordnete-wollen-manipulationstechniken-im-netz-verbieten/>
- Dr. Datenschutz:
<https://www.dr-datenschutz.de/deepfakes-betroffene-durch-kug-dsgvo-genuegend-geschuetzt/>



Social-Media-Kampagne: „KI-gestützte Chatbots und persönliche Assistenten“

Beitrag 1: Podcast-Ankündigung

- **Bild/Video:** Ein animiertes Bild mit dem Titel „Was weiß Siri über dich?“ und einem Play-Button.
- **Text (Post-Beschreibung):** „🎧 Wie viele Daten sammeln Siri, Alexa und Google Assistant wirklich über dich? In unserem neuen Podcast erfährst du, welche Daten gesammelt werden und wie du dich schützen kannst.
👉 Hör jetzt rein! #Sprachassistenten #BigData #Datenschutz #KI #DSGVO“

Beitrag 2: 2-Minuten-Video „Wie sicher sind deine Daten?“

- **Bild/Video:** Ein 2-minütiges Video, das eine Diskussion über die Privatsphäre-Risiken von Sprachassistenten zeigt.
- **Text (Post-Beschreibung):** „👁️ Weißt du, was Sprachassistenten über dich wissen? In unserem neuen Video erfährst du, wie diese Assistenten Daten sammeln und was du tun kannst, um deine Privatsphäre zu schützen. #KI #Sprachassistenten #Datenschutz #BigData #DSGVO“

Beitrag 3: Aufklärungsflyer

- **Bild:** Der Flyer über KI-gestützte Chatbots und persönliche Assistenten (siehe oben).
- **Text (Post-Beschreibung):** „📄 Lade unseren Flyer herunter und erfahre, wie KI-gestützte Assistenten deine Daten sammeln und wie du sie schützen kannst! #Flyer #Sprachassistenten #Datenschutz #BigData #DSGVO“

Zusätzliche Post-Ideen:

Post-Idee 1: Quiz zur Datensicherheit bei Sprachassistenten

- **Bild:** Ein interaktives Bild mit der Quiz-Frage: „Weißt du, was Siri und Alexa wirklich über dich sammeln?“ mit Antwortmöglichkeiten wie: „Ja, ich passe auf!“ oder „Nein, keine Ahnung!“
- **Text:** „Teste dein Wissen! Weißt du, wie du deine Sprachassistenten sicher nutzt? Nimm an unserem Quiz teil und finde es heraus! #Sprachassistenten #Datenschutz #KI #DSGVO“

Post-Idee 2: Fakten über KI-gestützte Chatbots und Datenschutz

- **Bild:** Eine Infografik mit Fakten zur Datensammlung durch Sprachassistenten, z.B.: „Sprachassistenten wie Siri, Alexa und Google Assistant hören immer zu, um deine Anfragen besser zu verstehen – aber wusstest du, dass sie auch deine Gespräche aufzeichnen können?“
- **Text:** „Schon gewusst? Sprachassistenten sammeln mehr Daten, als du denkst. Erfahre, wie du deine Privatsphäre schützen kannst! #Sprachassistenten #Datensicherheit #BigData #DSGVO“

Story-Idee: Umfrage zu Sprachassistenten und Datenschutz

- **Frage:** „Nutzt du Siri, Alexa oder Google Assistant? Weißt du, welche Daten sie über dich sammeln?“
- **Optionen:** „Ja, ich passe auf!“ / „Nein, keine Ahnung!“
- **Ergebnis:** Bei „Nein“ könnte ein Swipe-up-Link zu einem erklärenden Video oder einem Infopost geleitet werden.

Post-Idee 3: Tutorial zum Schutz deiner Daten bei Sprachassistenten

- **Bild:** Ein Bild eines Sprachassistenten mit einem Datenschutzsymbol daneben.
- **Text:** „Deine Daten sind wertvoll – auch für Sprachassistenten. In unserem Tutorial erfährst du, wie du die Datenschutz-Einstellungen bei Siri, Alexa und Google Assistant anpasst, um deine Daten zu schützen. #Sprachassistenten #Datenschutz #DSGVO #SicherImNetz“

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

PREDICTIVE POLICING

Predictive Policing bezeichnet den Einsatz von Algorithmen auf Basis von Big Data, um zukünftige Verbrechen vorherzusagen und Polizeiarbeit zu optimieren. Durch die Analyse großer Datenmengen vergangener Verbrechen, können Sicherheitsbehörden potenzielle Tatorte, Tatzeiten oder sogar Tatverdächtige identifizieren und damit gezielt "kriminalträchtige Orte, Personen oder Zeiten" benennen. Dabei werden auch Daten aus Social Media entnommen und analysiert. Dies birgt die Gefahr von Racial Profiling und wirft Datenschutzfragen auf.

PODCAST

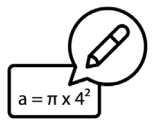
Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



PREDICTIVE POLICING



Verbrechen vorhersagen – hilfreich oder bedenklich?

Predictive Policing bezeichnet den Einsatz von Algorithmen und Big Data, um zukünftige Verbrechen vorherzusagen und Polizeiarbeit zu optimieren. Durch die Analyse großer Datenmengen – wie historische Kriminalitätsdaten, demografische Informationen und Geolokalisierungsdaten – können Polizei und Sicherheitsbehörden potenzielle Tatorte, Tatzeiten oder sogar Verdächtige identifizieren, bevor ein Verbrechen geschieht. Diese Technologie verspricht, die Effizienz der Strafverfolgung zu steigern, indem sie Polizeiressourcen gezielt auf „kriminalitätsstrchtige“ Orte lenkt. **Big Data** spielt dabei eine entscheidende Rolle: Je mehr Daten gesammelt und ausgewertet werden, desto genauer sollen die Vorhersagen über mögliche Verbrechen sein. Hierbei werden verschiedene Datenquellen, wie frühere Kriminalitätsberichte, soziale Medien, Überwachungskameras und sogar Wetterdaten, analysiert. Doch diese Entwicklung ist nicht ohne Kritik. Ein großes Problem im Zusammenhang mit Predictive Policing ist **Racial Profiling**. Kritiker argumentieren, dass die Algorithmen oft auf bereits verzerrten Daten basieren, die rassistische oder voreingenommene Muster reproduzieren. So könnten bestimmte ethnische Gruppen oder Stadtteile aufgrund ihrer historischen Kriminalitätsdaten überproportional oft als „gefährlich“ eingestuft werden, was zu einer verstärkten polizeilichen Überwachung führt. Dadurch entstehen Ungerechtigkeiten und die Gefahr, dass Diskriminierung verstärkt wird. Darüber hinaus wirft Predictive Policing ernsthafte **Datenschutzfragen** auf. Die riesigen Mengen an persönlichen Daten, die gesammelt und verarbeitet werden, betreffen nicht nur Kriminelle, sondern auch unbescholtene Bürger. Der Einsatz dieser Technologie könnte das Recht auf Privatsphäre untergraben und die Überwachung der Bevölkerung intensivieren, ohne dass klare Regulierungen festgelegt sind. In vielen Fällen sind Bürger sich nicht bewusst, dass ihre Daten verwendet werden, um Vorhersagen über potenzielle Verbrechen zu treffen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktioniert Predictive Policing und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO/EUMK schützen dich vor dem Missbrauch deiner Daten durch Predictive Policing?
- Welche Risiken bestehen durch die Nutzung von Predictive Policing für deine Privatsphäre?
- Wie trägt Predictive Policing zu Racial Profiling bei und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn Predictive Policing in deiner Stadt eingesetzt wird?

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



QR 1: Charta der Grundrechte der EU – Artikel 8 – Schutz personenbezogener Daten



QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: Europäische Menschenrechtskonvention – Artikel 8 – Recht auf Achtung des Privatlebens



QR 4: DSGVO Artikel 12 bis 22 z.B. Recht auf Auskunft, Recht auf Berechtigung, Recht auf Widerspruch



QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

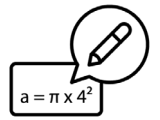


Weitere Quellen:

- Bund Deutscher Kriminalbeamter: <https://www.bdk.de/der-bdk/wer-wir-sind/positionen/2020-11-12-positionspapier-predictive-policing.pdf>
- Zukunftsinstitut: <https://www.zukunftsinstitut.de/zukunftsthemen/predictive-policing>
- Universität Hamburg: <https://www.wiso.uni-hamburg.de/fachbereich-sowi/ueber-den-fachbereich/fachgebiete/fachgebiet-kriminologische-sozialforschung/predictive-policing.html>
- Predictive Policing: <https://ksv-polizeipraxis.de/predictive-policing-umsetzung-und-wirkung-von-kriminalitaetsprognosen/>



PREDICTIVE POLICING



1. Podcast-Interviewer-Leitfaden (5-Minuten Podcast)

Frage 1:

„Was ist Predictive Policing und wie funktioniert es?“

(Ziel: Einführung in die Funktionsweise von Predictive Policing und die Rolle von Big Data.)

Frage 2:

„Welche Vorteile sehen Polizei und Sicherheitsbehörden im Einsatz von Predictive Policing?“

(Ziel: Darstellung der möglichen Effizienzgewinne und der präventiven Wirkung.)

Frage 3:

„Wo liegt die Grenze zwischen Sicherheit und Privatsphäre? Was passiert mit den gesammelten Daten der Bürger?“

(Ziel: Diskussion über Datenschutz und mögliche Verletzungen der Privatsphäre durch die Vorhersagetechnologie.)

Frage 4:

„Wie beeinflusst Predictive Policing ethnische Minderheiten, und warum ist Racial Profiling ein zentrales Problem?“

(Ziel: Vertiefung der Problematik von Racial Profiling und Diskriminierung durch auf Algorithmen basierende Polizeiarbeit.)

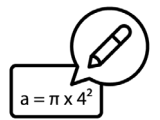
Frage 5:

„Wie könnte Predictive Policing in Zukunft reguliert werden, um Missbrauch zu verhindern und Grundrechte zu schützen?“

(Ziel: Diskussion über die Notwendigkeit von Regulierungen und Maßnahmen, um Datenschutz und Menschenrechte zu gewährleisten.)



PREDICTIVE POLICING



Verbrechen vorhersagen – hilfreich oder bedenklich?

Predictive Policing bezeichnet den Einsatz von Algorithmen und Big Data, um zukünftige Verbrechen vorherzusagen und Polizeiarbeit zu optimieren. Durch die Analyse großer Datenmengen – wie historische Kriminalitätsdaten, demografische Informationen und Geolokalisierungsdaten – können Polizei und Sicherheitsbehörden potenzielle Tatorte, Tatzeiten oder sogar Verdächtige identifizieren, bevor ein Verbrechen geschieht. Diese Technologie verspricht, die Effizienz der Strafverfolgung zu steigern, indem sie Polizeiressourcen gezielt auf „kriminalitätssträchtige“ Orte lenkt. **Big Data** spielt dabei eine entscheidende Rolle: Je mehr Daten gesammelt und ausgewertet werden, desto genauer sollen die Vorhersagen über mögliche Verbrechen sein. Hierbei werden verschiedene Datenquellen, wie frühere Kriminalitätsberichte, soziale Medien, Überwachungskameras und sogar Wetterdaten, analysiert. Doch diese Entwicklung ist nicht ohne Kritik. Ein großes Problem im Zusammenhang mit Predictive Policing ist **Racial Profiling**. Kritiker argumentieren, dass die Algorithmen oft auf bereits verzerrten Daten basieren, die rassistische oder voreingenommene Muster reproduzieren. So könnten bestimmte ethnische Gruppen oder Stadtteile aufgrund ihrer historischen Kriminalitätsdaten überproportional oft als „gefährlich“ eingestuft werden, was zu einer verstärkten polizeilichen Überwachung führt. Dadurch entstehen Ungerechtigkeiten und die Gefahr, dass Diskriminierung verstärkt wird. Darüber hinaus wirft Predictive Policing ernsthafte **Datenschutzfragen** auf. Die riesigen Mengen an persönlichen Daten, die gesammelt und verarbeitet werden, betreffen nicht nur Kriminelle, sondern auch unbescholtene Bürger. Der Einsatz dieser Technologie könnte das Recht auf Privatsphäre untergraben und die Überwachung der Bevölkerung intensivieren, ohne dass klare Regulierungen festgelegt sind. In vielen Fällen sind Bürger sich nicht bewusst, dass ihre Daten verwendet werden, um Vorhersagen über potenzielle Verbrechen zu treffen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktioniert Predictive Policing und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO/EUMK schützen dich vor dem Missbrauch deiner Daten durch Predictive Policing?
- Welche Risiken bestehen durch die Nutzung von Predictive Policing für deine Privatsphäre?
- Wie trägt Predictive Policing zu Racial Profiling bei und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn Predictive Policing in deiner Stadt eingesetzt wird?

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, das alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze iMovie/Clips zum Erstellen und Bearbeiten der Inhalte.



QR 1: Charta der Grundrechte der EU – Artikel 8 – Schutz personenbezogener Daten



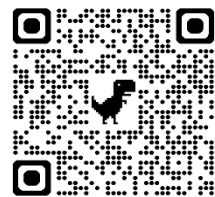
QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: Europäische Menschenrechtskonvention – Artikel 8 – Recht auf Achtung des Privatlebens



QR 4: DSGVO Artikel 12 bis 22 z.B. Recht auf Auskunft, Recht auf Berechtigung, Recht auf Widerspruch



QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

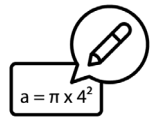


Weitere Quellen:

- Bund Deutscher Kriminalbeamter: <https://www.bdk.de/der-bdk/wer-wir-sind/positionen/2020-11-12-positionspapier-predictive-policing.pdf>
- Zukunftsinstitut: <https://www.zukunftsinstitut.de/zukunftsthemen/predictive-policing>
- Universität Hamburg: <https://www.wiso.uni-hamburg.de/fachbereich-sowi/ueber-den-fachbereich/fachgebiete/fachgebiet-kriminologische-sozialforschung/predictive-policing.html>
- Predictive Policing: <https://ksv-polizeipraxis.de/predictive-policing-umsetzung-und-wirkung-von-kriminalitaetsprognosen/>



PREDICTIVE POLICING



Szenenbeschreibung für ein 2-Minuten-Video

Titel: „Predictive Policing: Chance oder Risiko?“

Ort: Eine Stadt bei Nacht. Person A und Person B gehen durch ein belebtes Stadtviertel, während im Hintergrund Polizeiautos patrouillieren.

Person A (besorgt): „Hast du gehört? Die Polizei weiß jetzt schon, wo Verbrechen passieren werden – dank dieser neuen Vorhersagetechnologie.“

Person B (nachdenklich): „Ja, das nennt sich Predictive Policing. Klingt nützlich, aber ich frage mich, wie das funktioniert.“

Person A (erklärend): „Sie verwenden riesige Mengen an Daten – alte Kriminalitätsberichte, sogar das Wetter – um vorherzusagen, wo ein Verbrechen passieren könnte.“

Person B (skeptisch): „Aber was, wenn die Daten verzerrt sind? Was ist mit den Leuten, die aufgrund ihrer Herkunft oder ihres Viertels ins Visier geraten?“

Person A (nachdenklich): „Stimmt. Wenn die Daten auf alten Vorurteilen basieren, könnte das zu noch mehr Racial Profiling führen.“

Person B (ernst): „Ganz zu schweigen davon, dass unsere Daten möglicherweise ohne unser Wissen verwendet werden. Wie steht's mit unserem Recht auf Privatsphäre?“

Person A (zustimmend): „Ich denke, wir müssen wirklich darüber nachdenken, wie diese Technologie reguliert wird.“

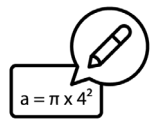
Schlusszene:

Text auf dem Bildschirm: „Predictive Policing: Effizienz oder Überwachung? Schütze deine Daten. #DSGVO #BigData #Privatsphäre“

Voiceover: „Informiere dich über Predictive Policing und seine Auswirkungen auf deine Rechte.“



PREDICTIVE POLICING



Verbrechen vorhersagen – hilfreich oder bedenklich?

Predictive Policing bezeichnet den Einsatz von Algorithmen und Big Data, um zukünftige Verbrechen vorherzusagen und Polizeiarbeit zu optimieren. Durch die Analyse großer Datenmengen – wie historische Kriminalitätsdaten, demografische Informationen und Geolokalisierungsdaten – können Polizei und Sicherheitsbehörden potenzielle Tatorte, Tatzeiten oder sogar Verdächtige identifizieren, bevor ein Verbrechen geschieht. Diese Technologie verspricht, die Effizienz der Strafverfolgung zu steigern, indem sie Polizeiressourcen gezielt auf „kriminalitätssträchtige“ Orte lenkt. **Big Data** spielt dabei eine entscheidende Rolle: Je mehr Daten gesammelt und ausgewertet werden, desto genauer sollen die Vorhersagen über mögliche Verbrechen sein. Hierbei werden verschiedene Datenquellen, wie frühere Kriminalitätsberichte, soziale Medien, Überwachungskameras und sogar Wetterdaten, analysiert. Doch diese Entwicklung ist nicht ohne Kritik. Ein großes Problem im Zusammenhang mit Predictive Policing ist **Racial Profiling**. Kritiker argumentieren, dass die Algorithmen oft auf bereits verzerrten Daten basieren, die rassistische oder voreingenommene Muster reproduzieren. So könnten bestimmte ethnische Gruppen oder Stadtteile aufgrund ihrer historischen Kriminalitätsdaten überproportional oft als „gefährlich“ eingestuft werden, was zu einer verstärkten polizeilichen Überwachung führt. Dadurch entstehen Ungerechtigkeiten und die Gefahr, dass Diskriminierung verstärkt wird. Darüber hinaus wirft Predictive Policing ernsthafte **Datenschutzfragen** auf. Die riesigen Mengen an persönlichen Daten, die gesammelt und verarbeitet werden, betreffen nicht nur Kriminelle, sondern auch unbescholtene Bürger. Der Einsatz dieser Technologie könnte das Recht auf Privatsphäre untergraben und die Überwachung der Bevölkerung intensivieren, ohne dass klare Regulierungen festgelegt sind. In vielen Fällen sind Bürger sich nicht bewusst, dass ihre Daten verwendet werden, um Vorhersagen über potenzielle Verbrechen zu treffen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktioniert Predictive Policing und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO/EUMK schützen dich vor dem Missbrauch deiner Daten durch Predictive Policing?
- Welche Risiken bestehen durch die Nutzung von Predictive Policing für deine Privatsphäre?
- Wie trägt Predictive Policing zu Racial Profiling bei und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn Predictive Policing in deiner Stadt eingesetzt wird?

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



QR 1: Charta der Grundrechte der EU – Artikel 8 – Schutz personenbezogener Daten



QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: Europäische Menschenrechtskonvention – Artikel 8 – Recht auf Achtung des Privatlebens



QR 4: DSGVO Artikel 12 bis 22 z.B. Recht auf Auskunft, Recht auf Berechtigung, Recht auf Widerspruch



QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

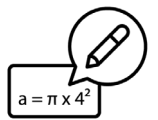


Weitere Quellen:

- Bund Deutscher Kriminalbeamter: <https://www.bdk.de/der-bdk/wer-wir-sind/positionen/2020-11-12-positionspapier-predictive-policing.pdf>
- Zukunftsinstitut: <https://www.zukunftsinstitut.de/zukunftsthemen/predictive-policing>
- Universität Hamburg: <https://www.wiso.uni-hamburg.de/fachbereich-sowi/ueber-den-fachbereich/fachgebiete/fachgebiet-kriminologische-sozialforschung/predictive-policing.html>
- Predictive Policing: <https://ksv-polizeipraxis.de/predictive-policing-umsetzung-und-wirkung-von-kriminalitaetsprognosen/>



PREDICTIVE POLICING



Flyer-Inhalt: „Schon gewusst?“ – Predictive Policing und Big Data (KI-generiert)

1. Überschrift:

- **Position:** Oben, zentriert.
- **Text:** „Schon gewusst?“ in großer, fetter Schrift.
- **Schriftart:** Moderne, klare Schriftart (z.B. Arial oder Helvetica).
- **Farbe:** Blau, um Aufmerksamkeit zu erregen.

2. Einleitender Text:

- **Position:** Direkt unter der Überschrift.
- **Text:** Eine kurze Erklärung, wie Predictive Policing mithilfe von Big Data Verbrechen vorhersagt und welche Risiken es für die Privatsphäre und das Problem des Racial Profiling mit sich bringt.
- **Schriftart:** Kleinere, gut lesbare Schrift.
- **Farbe:** Schwarz oder dunkles Grau.

3. Fakten und Tipps:

- **Position:** In der Mitte, als Liste angeordnet.
- **Text:** 3–4 Tipps, z.B.:
 - „Überprüfe deine Datenschutzeinstellungen.“
 - „Informiere dich über die Datennutzung in deiner Stadt.“
 - „Nutze dein Recht auf Auskunft gemäß DSGVO.“
 - „Setze dich für transparente Polizeiarbeit ein.“
- **Schriftart:** Leicht hervorgehoben (z.B. fett oder kursiv), damit die Tipps ins Auge fallen.
- **Farbe:** Schwarz für den Text, Blau für Aufzählungspunkte oder Nummern, um die Liste hervorzuheben.

4. Grafik/Symbol:

- **Position:** Unten rechts.
- **Bild:** Ein Symbol, das eine Polizeimarke und ein Datenschutzschild kombiniert.
- **Größe:** Dezent und klein, um den Text zu unterstreichen.

5. Abschlusssatz:

- **Position:** Unten links, neben der Grafik.
- **Text:** „Bleib informiert und schütze deine Daten. #DSGVO #PredictivePolicing #BigData.“
- **Schriftart:** Klein, aber gut lesbar.
- **Farbe:** Blau oder Grau, um sich harmonisch in das Design einzufügen.

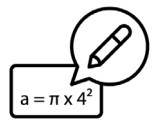
Gestaltungstipps:

- **Weißer Raum:** Nutze weißen Raum, um den Flyer nicht zu überladen und die Lesbarkeit zu erhöhen.
- **Symmetrie:** Eine symmetrische Anordnung hilft, das Design sauber und professionell wirken zu lassen.
- **Farbharmonie:** Verwende eine konsistente Farbpalette (Blau und Grau), um ein harmonisches Erscheinungsbild zu erzielen.
- **Klare Schriftarten:** Wähle gut lesbare Schriftarten für alle Textelemente, um die Verständlichkeit zu gewährleisten.





PREDICTIVE POLICING



Verbrechen vorhersagen – hilfreich oder bedenklich?

Predictive Policing bezeichnet den Einsatz von Algorithmen und Big Data, um zukünftige Verbrechen vorherzusagen und Polizeiarbeit zu optimieren. Durch die Analyse großer Datenmengen – wie historische Kriminalitätsdaten, demografische Informationen und Geolokalisierungsdaten – können Polizei und Sicherheitsbehörden potenzielle Tatorte, Tatzeiten oder sogar Verdächtige identifizieren, bevor ein Verbrechen geschieht. Diese Technologie verspricht, die Effizienz der Strafverfolgung zu steigern, indem sie Polizeiressourcen gezielt auf „kriminalitätssträchtige“ Orte lenkt. **Big Data** spielt dabei eine entscheidende Rolle: Je mehr Daten gesammelt und ausgewertet werden, desto genauer sollen die Vorhersagen über mögliche Verbrechen sein. Hierbei werden verschiedene Datenquellen, wie frühere Kriminalitätsberichte, soziale Medien, Überwachungskameras und sogar Wetterdaten, analysiert. Doch diese Entwicklung ist nicht ohne Kritik. Ein großes Problem im Zusammenhang mit Predictive Policing ist **Racial Profiling**. Kritiker argumentieren, dass die Algorithmen oft auf bereits verzerrten Daten basieren, die rassistische oder voreingenommene Muster reproduzieren. So könnten bestimmte ethnische Gruppen oder Stadtteile aufgrund ihrer historischen Kriminalitätsdaten überproportional oft als „gefährlich“ eingestuft werden, was zu einer verstärkten polizeilichen Überwachung führt. Dadurch entstehen Ungerechtigkeiten und die Gefahr, dass Diskriminierung verstärkt wird. Darüber hinaus wirft Predictive Policing ernsthafte **Datenschutzfragen** auf. Die riesigen Mengen an persönlichen Daten, die gesammelt und verarbeitet werden, betreffen nicht nur Kriminelle, sondern auch unbescholtene Bürger. Der Einsatz dieser Technologie könnte das Recht auf Privatsphäre untergraben und die Überwachung der Bevölkerung intensivieren, ohne dass klare Regulierungen festgelegt sind. In vielen Fällen sind Bürger sich nicht bewusst, dass ihre Daten verwendet werden, um Vorhersagen über potenzielle Verbrechen zu treffen.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktioniert Predictive Policing und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO/EUMK schützen dich vor dem Missbrauch deiner Daten durch Predictive Policing?
- Welche Risiken bestehen durch die Nutzung von Predictive Policing für deine Privatsphäre?
- Wie trägt Predictive Policing zu Racial Profiling bei und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn Predictive Policing in deiner Stadt eingesetzt wird?

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



QR 1: Charta der Grundrechte der EU – Artikel 8 – Schutz personenbezogener Daten



QR 2: DSGVO Art. 9 Verarbeitung personenbezogener Daten



QR 3: Europäische Menschenrechtskonvention – Artikel 8 – Recht auf Achtung des Privatlebens



QR 4: DSGVO Artikel 12 bis 22 z.B. Recht auf Auskunft, Recht auf Berechtigung, Recht auf Widerspruch



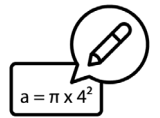
QR 5: DSGVO Art. 6 "Rechtmäßigkeit der Verarbeitung"

Weitere Quellen:

- Bund Deutscher Kriminalbeamter: <https://www.bdk.de/der-bdk/wer-wir-sind/positionen/2020-11-12-positionspapier-predictive-policing.pdf>
- Zukunftsinstitut: <https://www.zukunftsinstitut.de/zukunftsthemen/predictive-policing>
- Universität Hamburg: <https://www.wiso.uni-hamburg.de/fachbereich-sowi/ueber-den-fachbereich/fachgebiete/fachgebiet-kriminologische-sozialforschung/predictive-policing.html>
- Predictive Policing: <https://ksv-polizeipraxis.de/predictive-policing-umsetzung-und-wirkung-von-kriminalitaetsprognosen/>



PREDICTIVE POLICING



Beiträge der Kampagne:

Beitrag 1: Podcast-Ankündigung

Bild/Video: Ein animiertes Bild mit dem Titel „Predictive Policing: Was du wissen musst“ und einem Play-Button.

Text (Post-Beschreibung): „🎧 Weißt du, wie Big Data und KI genutzt werden, um Verbrechen vorherzusagen? Erfahre in unserem neuen Podcast, welche Auswirkungen Predictive Policing auf Datenschutz und Privatsphäre hat und wie Racial Profiling vermieden werden kann. ➡️ Hör jetzt rein! #PredictivePolicing #BigData #Datenschutz #DSGVO #Privatsphäre“

Beitrag 2: 2-Minuten-Video „Sicherheit oder Überwachung?“

Bild/Video: Ein 2-minütiges Video, das eine Unterhaltung über die Risiken und Chancen von Predictive Policing zeigt, insbesondere in Bezug auf Datenschutz und Racial Profiling.

Text (Post-Beschreibung): „👁️ Ist Predictive Policing ein Schritt in Richtung mehr Sicherheit oder fördert es Überwachung und Diskriminierung? In unserem neuen Video erfährst du, wie diese Technologie funktioniert und was du darüber wissen solltest! #PredictivePolicing #BigData #Datenschutz #DSGVO #RacialProfiling“

Beitrag 3: Aufklärungsflyer

Bild: Der Flyer über Predictive Policing und Datenschutz (siehe Beispiel-Flyer oben).

Text (Post-Beschreibung): „📄 Lade unseren Flyer herunter und erfahre, wie Predictive Policing funktioniert und wie du deine Daten und Rechte schützen kannst! #Flyer #PredictivePolicing #Datenschutz #BigData #DSGVO“

Zusätzliche Post-Ideen:

Post-Idee 1: Quiz zu Predictive Policing

Bild: Ein interaktives Bild mit der Quiz-Frage: „Weißt du, wie Predictive Policing deine Daten nutzt?“ mit Antwortmöglichkeiten wie: „Ja, ich bin informiert!“ oder „Nein, erzähl mir mehr!“.

Text: „Teste dein Wissen! Weißt du, welche Daten für Predictive Policing verwendet werden und welche Auswirkungen das auf dich haben kann? Nimm an unserem Quiz teil und finde es heraus! #PredictivePolicing #BigData #Quiz #Datenschutz #DSGVO“

Post-Idee 2: Fakten über Predictive Policing und Datenschutz

Bild: Eine Infografik mit Fakten zu Predictive Policing, z.B.: „Wusstest du, dass Predictive Policing das Risiko von Racial Profiling erhöhen kann? Informiere dich über deine Rechte und wie du deine Daten schützen kannst!“.

Text: „Schon gewusst? Predictive Policing nutzt große Datenmengen, um Verbrechen vorherzusagen, kann aber auch zu Diskriminierung führen. Erfahre, wie du deine Privatsphäre schützen kannst! #PredictivePolicing #Datensicherheit #BigData #DSGVO“

Story-Idee: Umfrage zu Predictive Policing und Privatsphäre

Frage: „Weißt du, wie deine persönlichen Daten von der Polizei genutzt werden? Fühlst du dich ausreichend geschützt?“

Optionen: „Ja, ich weiß es!“ / „Nein, keine Ahnung!“

Ergebnis: Bei „Nein“ könnte ein Swipe-up-Link zu einem erklärenden Video oder einem Infopost geleitet werden, der mehr Informationen über Predictive Policing und Datenschutz bietet.

Post-Idee 3: Tutorial zum Schutz deiner Daten

Bild: Ein Bild von einem Datenschutzsymbol und einem Polizeiemblem, das die Balance zwischen Sicherheit und Privatsphäre darstellt.

Text: „Deine Daten sind wertvoll – auch für Predictive Policing. Erfahre in unserem Tutorial, wie du deine Datenschutzrechte wahrnehmen und dich vor ungerechtfertigter Überwachung schützen kannst! #PredictivePolicing #Datenschutz #DSGVO #SicherheitImNetz“

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

SMARTE MOBILITÄT

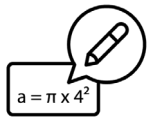
Die Automobilindustrie erlebt einen tiefgreifenden Wandel durch die Integration von smarten Technologien und KI in Fahrzeuge. Smarte Fahrzeuge, Sprachassistenten und Connected Cars greifen auf die Sensoren, Kameras, GPS-Daten und andere Technologien des Autos zurück, um das Fahrverhalten zu analysieren und sicherheitsoptimierte Änderungen in ihren Fahrzeugen vorzunehmen. Dabei spielt auch die Versicherungsbranche mit Telematik-Tarifen eine Rolle. Doch inwieweit wird sichergestellt, dass die gesammelten Daten nur für die Fahrzeuganalyse genutzt wird?

PODCAST

Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



Smarte Mobilität – Kameras, Sensoren und GPS

Die Automobilindustrie erlebt einen tiefgreifenden Wandel durch die Integration von **smarten Technologien** in Fahrzeuge. **Smarte Fahrzeuge** oder **Connected Cars** sind Autos, die mit dem Internet verbunden sind und Daten in Echtzeit senden und empfangen können. Diese Fahrzeuge nutzen Sensoren, Kameras, GPS und andere Technologien, um Informationen zu sammeln, die das Fahrerlebnis verbessern sollen. Dazu gehören Navigationsdienste, Verkehrsflussanalysen, Fahrassistenzsysteme und personalisierte Entertainment-Angebote. **Big Data** spielt dabei eine entscheidende Rolle. Die riesigen Datenmengen, die von smarten Fahrzeugen generiert werden, ermöglichen es Herstellern und Drittanbietern, detaillierte Einblicke in das Fahrverhalten, die Fahrzeugnutzung und die Vorlieben der Nutzer zu erhalten. Diese Daten können verwendet werden, um Dienstleistungen zu optimieren, neue Geschäftsmodelle zu entwickeln oder sogar Wartung und Sicherheit zu verbessern. Ein wichtiges Beispiel für die Nutzung dieser Daten ist die **Versicherungsbranche**. **Versicherungsunternehmen** bieten zunehmend sogenannte **Telematik-Tarife** an, bei denen die Versicherungsprämien auf Basis des individuellen Fahrverhaltens berechnet werden. Daten wie Geschwindigkeit, Beschleunigungs- und Bremsverhalten, Fahrzeiten und zurückgelegte Strecken werden gesammelt und analysiert. Fahrer, die sicher und defensiv fahren, können so von günstigeren Tarifen profitieren. Allerdings bedeutet dies auch, dass Fahrer mit riskanterem Fahrverhalten höhere Prämien zahlen müssen. Diese Entwicklung wirft erhebliche **Datenschutzrisiken** auf. Persönliche Daten wie Standortinformationen, Fahrgeohnheiten oder sogar biometrische Daten können gesammelt und potenziell missbraucht werden. Es besteht die Gefahr, dass sensible Informationen ohne ausreichende Einwilligung der Nutzer an Dritte weitergegeben oder für andere Zwecke verwendet werden, als ursprünglich vorgesehen. Hier greift die **Datenschutz-Grundverordnung (DSGVO)** der EU ein, die den Schutz personenbezogener Daten regelt. Die DSGVO stellt sicher, dass Nutzer die Kontrolle über ihre Daten behalten, indem sie Rechte wie das **Recht auf Auskunft**, **Recht auf Löschung** und **Recht auf Widerspruch** bietet.



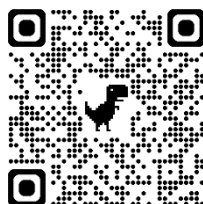
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren smarte Fahrzeuge und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch smarte Fahrzeuge und Versicherungen?
- Welche Risiken bestehen durch die Nutzung von smarten Fahrzeugen für deine Privatsphäre?
- Wie nutzen Versicherungen und Fahrzeughersteller die gesammelten Daten aus smarten Fahrzeugen, und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn du ein smartes Fahrzeug nutzt?

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



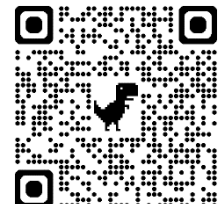
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



QR 4: Recht am
eigenen Bild

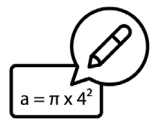


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- AutomotiveIT:
<https://www.automotiveit.eu/technology/die-data-journey-hat-begonnen-867.html>
- Bain.com:
<https://www.bain.com/de/insights/big-data-in-the-automotive-industry/>
- Springer Professional:
<https://www.springerprofessional.de/datensicherheit/big-data/das-vernetzte-auto-fordert-den-datenschutz-heraus/10860880>
- Autohaus.de:
<https://www.autohaus.de/nachrichten/autohandel/zwischen-datenschutz-und-it-security-3376162>



Podcast-Interviewer-Leitfaden (5-Minuten Podcast)

Frage 1:

Was sind smarte Fahrzeuge und welche Daten sammeln sie?

Ziel: Einführung in die Welt der vernetzten Autos und welche Arten von Daten (z.B. Standort, Fahrverhalten, Kommunikationsdaten) sie erfassen.

Frage 2:

Wie nutzen Automobilhersteller und Drittanbieter wie Versicherungen die gesammelten Daten aus smarten Fahrzeugen?

Ziel: Erklärung der Verwendung der Daten für Serviceverbesserungen, personalisierte Angebote und die Anpassung von Versicherungstarifen durch Telematik-Tarife.

Frage 3:

Welche Auswirkungen hat die Datennutzung durch Versicherungen auf die Fahrer? Ist das fair?

Ziel: Diskussion über die Vor- und Nachteile von Telematik-Tarifen, Datenschutzbedenken und mögliche Diskriminierung von Fahrern aufgrund ihres Fahrverhaltens.

Frage 4:

Welche Risiken bestehen generell für die Privatsphäre der Fahrer durch die Datensammlung in smarten Fahrzeugen?

Ziel: Vertiefung der Datenschutzthemen, einschließlich Datenmissbrauch, Weitergabe an Dritte und das Risiko von Hackerangriffen.

Frage 5:

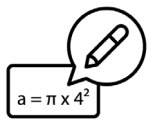
Wie schützt die DSGVO die Nutzer von smarten Fahrzeugen, und welche Rechte haben sie in Bezug auf ihre Daten?

Ziel: Erläuterung der relevanten DSGVO-Artikel, z.B. Recht auf Auskunft, Recht auf Löschung, und wie diese im Kontext von Fahrzeug- und Versicherungsdaten angewendet werden.

Frage 6:

Welche Maßnahmen können Fahrer ergreifen, um ihre Daten zu schützen und sicherzustellen, dass ihre Privatsphäre gewahrt bleibt, insbesondere im Hinblick auf Versicherungen?

Ziel: Praktische Tipps und Empfehlungen, wie Nutzer Datenschutzeinstellungen anpassen, Einwilligungen verwalten und bewusst mit vernetzten Diensten umgehen können.



Smarte Mobilität – Kameras, Sensoren und GPS

Die Automobilindustrie erlebt einen tiefgreifenden Wandel durch die Integration von **smarten Technologien** in Fahrzeuge. **Smarte Fahrzeuge** oder **Connected Cars** sind Autos, die mit dem Internet verbunden sind und Daten in Echtzeit senden und empfangen können. Diese Fahrzeuge nutzen Sensoren, Kameras, GPS und andere Technologien, um Informationen zu sammeln, die das Fahrerlebnis verbessern sollen. Dazu gehören Navigationsdienste, Verkehrsflussanalysen, Fahrassistenzsysteme und personalisierte Entertainment-Angebote. **Big Data** spielt dabei eine entscheidende Rolle. Die riesigen Datenmengen, die von smarten Fahrzeugen generiert werden, ermöglichen es Herstellern und Drittanbietern, detaillierte Einblicke in das Fahrverhalten, die Fahrzeugnutzung und die Vorlieben der Nutzer zu erhalten. Diese Daten können verwendet werden, um Dienstleistungen zu optimieren, neue Geschäftsmodelle zu entwickeln oder sogar Wartung und Sicherheit zu verbessern. Ein wichtiges Beispiel für die Nutzung dieser Daten ist die **Versicherungsbranche**. **Versicherungsunternehmen** bieten zunehmend sogenannte **Telematik-Tarife** an, bei denen die Versicherungsprämien auf Basis des individuellen Fahrverhaltens berechnet werden. Daten wie Geschwindigkeit, Beschleunigungs- und Bremsverhalten, Fahrzeiten und zurückgelegte Strecken werden gesammelt und analysiert. Fahrer, die sicher und defensiv fahren, können so von günstigeren Tarifen profitieren. Allerdings bedeutet dies auch, dass Fahrer mit riskanterem Fahrverhalten höhere Prämien zahlen müssen. Diese Entwicklung wirft erhebliche **Datenschutzrisiken** auf. Persönliche Daten wie Standortinformationen, Fahrgewohnheiten oder sogar biometrische Daten können gesammelt und potenziell missbraucht werden. Es besteht die Gefahr, dass sensible Informationen ohne ausreichende Einwilligung der Nutzer an Dritte weitergegeben oder für andere Zwecke verwendet werden, als ursprünglich vorgesehen. Hier greift die **Datenschutz-Grundverordnung (DSGVO)** der EU ein, die den Schutz personenbezogener Daten regelt. Die DSGVO stellt sicher, dass Nutzer die Kontrolle über ihre Daten behalten, indem sie Rechte wie das **Recht auf Auskunft**, **Recht auf Löschung** und **Recht auf Widerspruch** bietet.



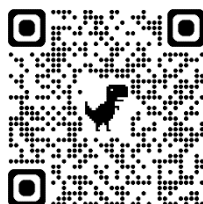
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren smarte Fahrzeuge und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch smarte Fahrzeuge und Versicherungen?
- Welche Risiken bestehen durch die Nutzung von smarten Fahrzeugen für deine Privatsphäre?
- Wie nutzen Versicherungen und Fahrzeughersteller die gesammelten Daten aus smarten Fahrzeugen, und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn du ein smartes Fahrzeug nutzt?

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, das alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze iMovie/Clips zum Erstellen und Bearbeiten der Inhalte.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



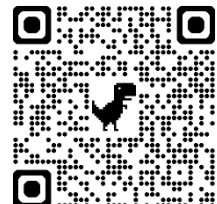
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



QR 4: Recht am
eigenen Bild

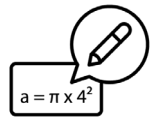


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- AutomotiveIT:
<https://www.automotiveit.eu/technology/die-data-journey-hat-begonnen-867.html>
- Bain.com:
<https://www.bain.com/de/insights/big-data-in-the-automotive-industry/>
- Springer Professional:
<https://www.springerprofessional.de/datensicherheit/big-data/das-vernetzte-auto-fordert-den-datenschutz-heraus/10860880>
- Autohaus.de:
<https://www.autohaus.de/nachrichten/autohandel/zwischen-datenschutz-und-it-security-3376162>



Szenenbeschreibung für einen 2-Minuten-Clip

Titel: „Dein Auto, deine Daten – Wer profitiert wirklich?“

Ort: Eine moderne Stadtstraße. Person A steigt in ihr smartes Fahrzeug ein, während Person B daneben steht.

Person A (freudig): „Schau mal, mein neues Auto ist echt genial! Es bietet mir sogar einen Rabatt auf meine Versicherung, weil es mein Fahrverhalten analysiert.“

Person B (nachdenklich): „Interessant, aber hast du dir mal Gedanken darüber gemacht, welche Daten dafür gesammelt werden?“

Person A (überrascht): „Naja, nur wie ich fahre, oder? Ist doch gut, wenn ich dadurch Geld spare.“

Person B (ernst): „Sie sammeln Daten über deine Geschwindigkeit, Beschleunigung, Bremsverhalten, wo und wann du fährst. Diese Daten gehen an deine Versicherung und wer weiß, an wen noch.“

Person A (besorgt): „Oh, daran habe ich nicht gedacht. Was passiert, wenn sie diese Daten gegen mich verwenden?“

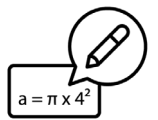
Person B (erklärend): „Genau das ist das Problem. Sie könnten deine Prämien erhöhen, wenn du mal schneller fährst, oder die Daten an Dritte weitergeben. Außerdem besteht immer das Risiko, dass diese sensiblen Daten in falsche Hände geraten.“

Person A (entschlossen): „Das klingt nicht gut. Was kann ich tun, um meine Daten zu schützen und trotzdem von den Vorteilen zu profitieren?“

Person B (ermutigend): „Du könntest genau prüfen, welche Daten du freigibst, die Datenschutzerklärungen lesen und deine Rechte gemäß DSGVO wahrnehmen. Manchmal ist es besser, auf solche Tarife zu verzichten, wenn sie zu viel Einblick in deine Privatsphäre verlangen.“

Schlusszene:

- **Text auf dem Bildschirm:** „Bleib informiert und schütze deine Privatsphäre im Straßenverkehr. #DSGVO #SmarteFahrzeuge #Versicherung #Datenschutz“
- **Voiceover:** „Erfahre mehr darüber, wie du deine Daten in smarten Fahrzeugen schützen kannst.“



Smarte Mobilität – Kameras, Sensoren und GPS

Die Automobilindustrie erlebt einen tiefgreifenden Wandel durch die Integration von **smarten Technologien** in Fahrzeuge. **Smarte Fahrzeuge** oder **Connected Cars** sind Autos, die mit dem Internet verbunden sind und Daten in Echtzeit senden und empfangen können. Diese Fahrzeuge nutzen Sensoren, Kameras, GPS und andere Technologien, um Informationen zu sammeln, die das Fahrerlebnis verbessern sollen. Dazu gehören Navigationsdienste, Verkehrsflussanalysen, Fahrassistenzsysteme und personalisierte Entertainment-Angebote. **Big Data** spielt dabei eine entscheidende Rolle. Die riesigen Datenmengen, die von smarten Fahrzeugen generiert werden, ermöglichen es Herstellern und Drittanbietern, detaillierte Einblicke in das Fahrverhalten, die Fahrzeugnutzung und die Vorlieben der Nutzer zu erhalten. Diese Daten können verwendet werden, um Dienstleistungen zu optimieren, neue Geschäftsmodelle zu entwickeln oder sogar Wartung und Sicherheit zu verbessern. Ein wichtiges Beispiel für die Nutzung dieser Daten ist die **Versicherungsbranche**. **Versicherungsunternehmen** bieten zunehmend sogenannte **Telematik-Tarife** an, bei denen die Versicherungsprämien auf Basis des individuellen Fahrverhaltens berechnet werden. Daten wie Geschwindigkeit, Beschleunigungs- und Bremsverhalten, Fahrzeiten und zurückgelegte Strecken werden gesammelt und analysiert. Fahrer, die sicher und defensiv fahren, können so von günstigeren Tarifen profitieren. Allerdings bedeutet dies auch, dass Fahrer mit riskanterem Fahrverhalten höhere Prämien zahlen müssen. Diese Entwicklung wirft erhebliche **Datenschutzrisiken** auf. Persönliche Daten wie Standortinformationen, Fahrgewohnheiten oder sogar biometrische Daten können gesammelt und potenziell missbraucht werden. Es besteht die Gefahr, dass sensible Informationen ohne ausreichende Einwilligung der Nutzer an Dritte weitergegeben oder für andere Zwecke verwendet werden, als ursprünglich vorgesehen. Hier greift die **Datenschutz-Grundverordnung (DSGVO)** der EU ein, die den Schutz personenbezogener Daten regelt. Die DSGVO stellt sicher, dass Nutzer die Kontrolle über ihre Daten behalten, indem sie Rechte wie das **Recht auf Auskunft**, **Recht auf Löschung** und **Recht auf Widerspruch** bietet.



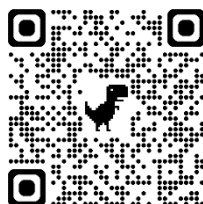
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren smarte Fahrzeuge und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch smarte Fahrzeuge und Versicherungen?
- Welche Risiken bestehen durch die Nutzung von smarten Fahrzeugen für deine Privatsphäre?
- Wie nutzen Versicherungen und Fahrzeughersteller die gesammelten Daten aus smarten Fahrzeugen, und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn du ein smartes Fahrzeug nutzt?

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



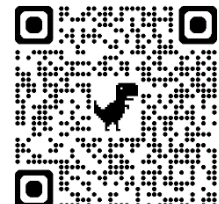
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



QR 4: Recht am
eigenen Bild

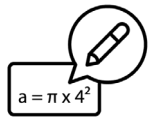


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- AutomotiveIT:
<https://www.automotiveit.eu/technology/die-data-journey-hat-begonnen-867.html>
- Bain.com:
<https://www.bain.com/de/insights/big-data-in-the-automotive-industry/>
- Springer Professional:
<https://www.springerprofessional.de/datensicherheit/big-data/das-vernetzte-auto-fordert-den-datenschutz-heraus/10860880>
- Autohaus.de:
<https://www.autohaus.de/nachrichten/autohandel/zwischen-datenschutz-und-it-security-3376162>



Flyer-Design: „Schon gewusst?“ – Smarte Fahrzeuge, Versicherungen und Datenschutz (KI generiert)

Flyer-Inhalt:

1. Überschrift:

- **Position:** Oben, zentriert.
- **Text:** „Schon gewusst?“ in großer, fetter Schrift.
- **Schriftart:** Moderne, klare Schriftart (z.B. Arial oder Helvetica).
- **Farbe:** Blau, um Aufmerksamkeit zu erregen.

2. Einleitender Text:

- **Position:** Direkt unter der Überschrift.
- **Text:** Eine kurze Erklärung, wie smarte Fahrzeuge Daten sammeln, die von Versicherungen genutzt werden können, um Tarife zu verändern, und welche Auswirkungen das auf deine Privatsphäre haben kann.
- **Schriftart:** Kleinere, gut lesbare Schrift.
- **Farbe:** Schwarz oder dunkles Grau.

3. Fakten und Tipps:

- **Position:** In der Mitte, als Liste angeordnet.
- **Text:** 3–4 Tipps, z.B.:
 - „Überprüfe die Datenschutzeinstellungen deines Fahrzeugs.“
 - „Sei vorsichtig mit der Freigabe von Fahrdaten an Versicherungen.“
 - „Lies die Datenschutzbestimmungen, bevor du Telematik-Tarife abschließt.“
 - „Nutze dein Recht auf Auskunft und Löschung gemäß DSGVO.“
- **Schriftart:** Leicht hervorgehoben (z.B. fett oder kursiv), damit die Tipps ins Auge fallen.
- **Farbe:** Schwarz für den Text, Blau für Aufzählungspunkte oder Nummern.

4. Grafik/Symbol:

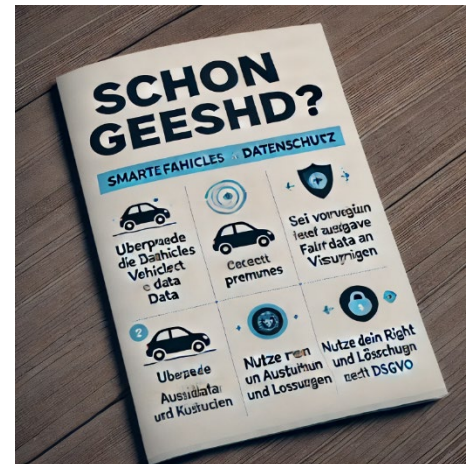
- **Position:** Unten rechts.
- **Bild:** Ein Symbol eines Autos mit einem Datenschutzschild oder einem Schloss, neben einem Versicherungssymbol (z.B. ein Schild oder Regenschirm).
- **Größe:** Dezent und klein, um den Text zu unterstreichen.

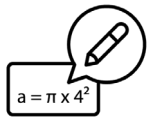
5. Abschlusssatz:

- **Position:** Unten links, neben der Grafik.
- **Text:** „Bleib informiert und schütze deine Daten auf der Straße. #DSGVO #SmarteFahrzeuge #Versicherung #Datenschutz“
- **Schriftart:** Klein, aber gut lesbar.
- **Farbe:** Blau oder Grau, um sich harmonisch in das Design einzufügen.

Gestaltungstipps:

- Nutze weißen Raum, um den Flyer nicht zu überladen.
- Symmetrische Anordnung hilft, das Design sauber und professionell wirken zu lassen.





Smarte Mobilität – Kameras, Sensoren und GPS

Die Automobilindustrie erlebt einen tiefgreifenden Wandel durch die Integration von **smarten Technologien** in Fahrzeuge. **Smarte Fahrzeuge** oder **Connected Cars** sind Autos, die mit dem Internet verbunden sind und Daten in Echtzeit senden und empfangen können. Diese Fahrzeuge nutzen Sensoren, Kameras, GPS und andere Technologien, um Informationen zu sammeln, die das Fahrerlebnis verbessern sollen. Dazu gehören Navigationsdienste, Verkehrsflussanalysen, Fahrassistenzsysteme und personalisierte Entertainment-Angebote. **Big Data** spielt dabei eine entscheidende Rolle. Die riesigen Datenmengen, die von smarten Fahrzeugen generiert werden, ermöglichen es Herstellern und Drittanbietern, detaillierte Einblicke in das Fahrverhalten, die Fahrzeugnutzung und die Vorlieben der Nutzer zu erhalten. Diese Daten können verwendet werden, um Dienstleistungen zu optimieren, neue Geschäftsmodelle zu entwickeln oder sogar Wartung und Sicherheit zu verbessern. Ein wichtiges Beispiel für die Nutzung dieser Daten ist die **Versicherungsbranche**. **Versicherungsunternehmen** bieten zunehmend sogenannte **Telematik-Tarife** an, bei denen die Versicherungsprämien auf Basis des individuellen Fahrverhaltens berechnet werden. Daten wie Geschwindigkeit, Beschleunigungs- und Bremsverhalten, Fahrzeiten und zurückgelegte Strecken werden gesammelt und analysiert. Fahrer, die sicher und defensiv fahren, können so von günstigeren Tarifen profitieren. Allerdings bedeutet dies auch, dass Fahrer mit riskanterem Fahrverhalten höhere Prämien zahlen müssen. Diese Entwicklung wirft erhebliche **Datenschutzrisiken** auf. Persönliche Daten wie Standortinformationen, Fahrgewohnheiten oder sogar biometrische Daten können gesammelt und potenziell missbraucht werden. Es besteht die Gefahr, dass sensible Informationen ohne ausreichende Einwilligung der Nutzer an Dritte weitergegeben oder für andere Zwecke verwendet werden, als ursprünglich vorgesehen. Hier greift die **Datenschutz-Grundverordnung (DSGVO)** der EU ein, die den Schutz personenbezogener Daten regelt. Die DSGVO stellt sicher, dass Nutzer die Kontrolle über ihre Daten behalten, indem sie Rechte wie das **Recht auf Auskunft**, **Recht auf Löschung** und **Recht auf Widerspruch** bietet.



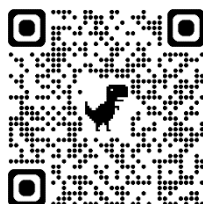
Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Wie funktionieren smarte Fahrzeuge und welche Rolle spielt Big Data dabei?
- Welche Regeln der DSGVO schützen dich vor dem Missbrauch deiner Daten durch smarte Fahrzeuge und Versicherungen?
- Welche Risiken bestehen durch die Nutzung von smarten Fahrzeugen für deine Privatsphäre?
- Wie nutzen Versicherungen und Fahrzeughersteller die gesammelten Daten aus smarten Fahrzeugen, und welche rechtlichen Folgen hat das?
- Wie kannst du deine Daten schützen und deine Rechte wahrnehmen, wenn du ein smartes Fahrzeug nutzt?

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



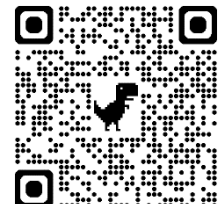
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



QR 4: Recht am
eigenen Bild



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- AutomotiveIT:
<https://www.automotiveit.eu/technology/die-data-journey-hat-begonnen-867.html>
- Bain.com:
<https://www.bain.com/de/insights/big-data-in-the-automotive-industry/>
- Springer Professional:
<https://www.springerprofessional.de/datensicherheit/big-data/das-vernetzte-auto-fordert-den-datenschutz-heraus/10860880>
- Autohaus.de:
<https://www.autohaus.de/nachrichten/autohandel/zwischen-datenschutz-und-it-security-3376162>



Social-Media-Kampagne: Smarte Fahrzeuge, Versicherungen und Datenschutz

Beitrag 1: Podcast-Ankündigung

- **Bild/Video:** Ein animiertes Bild mit dem Titel „Smarte Fahrzeuge und Versicherungen: Was du wissen musst“ und einem Play-Button.
- **Text (Post-Beschreibung):** „🎧 Dein Auto sammelt Daten, deine Versicherung kann sie nutzen. Erfahre in unserem neuen Podcast, wie smarte Fahrzeuge und Telematik-Tarife funktionieren und was das für deine Privatsphäre bedeutet. ➡ Hör jetzt rein! #SmarteFahrzeuge #Versicherung #BigData #Datenschutz #DSGVO“

Beitrag 2: 2-Minuten-Video „Daten auf der Überholspur?“

- **Bild/Video:** Ein 2-minütiges Video, das eine Unterhaltung über die Datensammlung in smarten Fahrzeugen und deren Nutzung durch Versicherungen zeigt.
- **Text (Post-Beschreibung):** „👁️ Deine Fahrdaten könnten deinen Versicherungsbeitrag beeinflussen! In unserem neuen Video erfährst du, wie Versicherungen Daten nutzen und was du tun kannst, um deine Privatsphäre zu schützen. #SmarteFahrzeuge #Versicherung #BigData #Datenschutz #DSGVO“

Beitrag 3: Aufklärungsflyer

- **Bild:** Der Flyer über smarte Fahrzeuge, Versicherungen und Datenschutz.
- **Text (Post-Beschreibung):** „📄 Lade unseren Flyer herunter und erfahre, wie du deine Daten im vernetzten Auto schützen und bewusst mit Telematik-Tarifen umgehen kannst! #Flyer #SmarteFahrzeuge #Versicherung #Datenschutz #BigData #DSGVO“

Zusätzliche Post-Ideen:

Post-Idee 1: Quiz zu Daten und Versicherungen

- **Bild:** Ein interaktives Bild mit der Quiz-Frage: „Weißt du, welche Daten deine Versicherung von dir erhält?“ mit Antwortmöglichkeiten wie: „Ja, voll im Bilde!“ oder „Nein, erzähl mir mehr!“
- **Text:** „Teste dein Wissen! Weißt du, welche Daten durch Telematik-Tarife gesammelt werden und was das für dich bedeutet? Nimm an unserem Quiz teil und finde es heraus! #SmarteFahrzeuge #Versicherung #Quiz #Datenschutz #DSGVO“

Post-Idee 2: Fakten über smarte Fahrzeuge, Versicherungen und Datenschutz

- **Bild:** Eine Infografik mit Fakten zu Telematik-Tarifen, z.B.: „Wusstest du, dass deine Fahrdaten deine Versicherungsprämie erhöhen oder senken können? Lerne, wie du deine Daten schützt!“
- **Text:** „Schon gewusst? Versicherungen nutzen Fahrdaten aus smarten Fahrzeugen zur Tarifgestaltung. Erfahre, wie du die Kontrolle behältst und deine Privatsphäre schützt! #SmarteFahrzeuge #Versicherung #Datensicherheit #BigData #DSGVO“

Story-Idee: Umfrage zu Telematik-Tarifen und Privatsphäre

- **Frage:** „Hast du einen Telematik-Tarif bei deiner Autoversicherung? Weißt du, welche Daten dabei gesammelt werden?“
- **Optionen:** „Ja, und ich bin informiert!“ / „Nein, keine Ahnung!“
- **Ergebnis:** Bei „Nein“ könnte ein Swipe-up-Link zu einem erklärenden Video oder einem Infopost geleitet werden.

Post-Idee 3: Tutorial zum Schutz deiner Daten bei Telematik-Tarifen

- **Bild:** Ein Bild eines Autos mit einem Schloss oder Datenschutzsymbol und einem Versicherungslogo.
- **Text:** „Deine Daten sind wertvoll – auch für Versicherungen. Erfahre in unserem Tutorial, wie du verantwortungsbewusst mit Telematik-Tarifen umgehst und deine Privatsphäre schützt! #SmarteFahrzeuge #Versicherung #Datenschutz #DSGVO #SicherImAuto“

SOCIAL MEDIA KAMPAGNE

Erstelle eine Social-Media Kampagne auf Instagram (fiktiv), in der du die Ergebnisse der anderen Gruppe in Szene stellst. Erstelle passende Stories, Posts, Reels und Umfragen.

FLYER

Gestalte einen "Schon gewusst?"-Flyer zu dem Thema. Bringe eigene Ideen und Gestaltungen ein. Was muss alles auf dem Flyer sein? Verlinke auch wichtige Gesetztestexte per QR-Code. Nutze Freeform oder SketchesSchool für den Entwurf.

SMART HOME UND IOT

Das Internet of Things ist in modernen Häusern nicht mehr wegzudenken. Smarte Geräte wie Beleuchtungssysteme, Haushaltsgeräte, uvm. begleiten passiv den Alltag von Menschen. Dabei werden die Nutzungsdaten dieser Geräte ständig gesammelt und ausgewertet. Inwieweit stellen also beispielsweise Bewegungssensoren oder Beleuchtung vielleicht ein Sicherheitsrisiko dar, wenn man ständig weiß, wann jemand sich im Haus befindet?

PODCAST

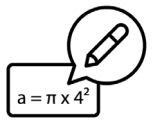
Erstelle einen kurzen Podcast (5 Minuten), der alles Relevante zum Thema erklärt. Es bietet sich ein Interview-Podcast an. Bereite den Podcast vor und nimm ihn z.B. über Audacity auf.

VIDEOSZENE

Erstelle ein kurzes Video (Clip), in dem alles Relevante zum Thema vorkommt. Stelle die rechtliche Lage dar und bringe eigene Ideen ein. Sprich das Publikum direkt an! Nutze iMovie/Clips zum Drehen und Schneiden.



SMART HOME UND IOT



Smart Home und IoT – wer hört alles zu?

Smart Home und das Internet der Dinge (IoT) – Vernetzte Haushalte, Big Data und Datenschutz

Das Konzept des Smart Homes beschreibt ein Zuhause, in dem verschiedene Geräte und Systeme über das Internet miteinander verbunden sind und automatisch oder per Fernsteuerung bedient werden können. Dazu gehören smarte Thermostate, Beleuchtungssysteme, Überwachungskameras, intelligente Lautsprecher und Haushaltsgeräte wie Kühlschränke und Waschmaschinen. Durch die Nutzung von Sensoren und Vernetzung ermöglichen Smart Homes eine verbesserte Kontrolle und Effizienz im Alltag. **Big Data** spielt auch hier eine entscheidende Rolle. Die in einem Smart Home generierten Daten bieten Einblicke in das Nutzerverhalten, zum Beispiel in Bezug auf Energieverbrauch, Gewohnheiten oder Sicherheitsbedürfnisse. Unternehmen können diese Daten nutzen, um ihre Produkte zu verbessern oder gezielte Dienstleistungen anzubieten. Besonders relevant sind dabei auch personalisierte Dienste, die auf den individuellen Vorlieben der Nutzer basieren. Ein Beispiel für die Nutzung von Daten in Smart Homes ist der Energiemarkt. Intelligente Stromzähler (Smart Meter) sammeln Daten über den Energieverbrauch und ermöglichen es, den Energieeinsatz effizienter zu gestalten oder Tarife dynamisch anzupassen. Allerdings bedeutet dies auch, dass Energieversorger detaillierte Informationen über den Alltag ihrer Kunden erhalten. Diese Entwicklungen werfen Fragen hinsichtlich des Datenschutzes auf. Geräte, die ständig Daten über unsere Aktivitäten sammeln, bergen das Risiko von Missbrauch oder unerlaubtem Zugriff. Zudem könnten sensible Informationen ohne ausreichende Einwilligung an Dritte weitergegeben oder für andere Zwecke verwendet werden. Die **Datenschutz-Grundverordnung (DSGVO)** der EU ist auch hier relevant und sichert den Schutz personenbezogener Daten. Nutzer haben das Recht zu wissen, welche Daten gesammelt werden, und können verlangen, dass diese gelöscht oder nicht mehr verwendet werden.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind Smart Homes und welche Daten sammeln sie?
- Wie nutzen Unternehmen und Drittanbieter die gesammelten Daten aus Smart Homes?
- Welche Auswirkungen hat die Datennutzung durch Unternehmen auf die Bewohner von Smart Homes? Ist das fair?
- Welche Risiken bestehen für die Privatsphäre der Bewohner durch die Datensammlung in Smart Homes?
- Wie schützt die DSGVO die Nutzer von Smart Homes, und welche Rechte haben sie in Bezug auf ihre Daten?
- Welche Maßnahmen können Nutzer ergreifen, um ihre Daten in einem Smart Home zu schützen?

Aufgabe 2: Erstelle einen 5-Minuten-Podcast zu dem Thema, der alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Einige Leitfragen findest du auf der Rückseite. Du kannst auch eigene Fragen einbringen. Nutze die Sprachmemo-Funktion zur Aufnahme einzelner Abschnitte. Füge sie anschließend in Audacity (Laptop) zusammen.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



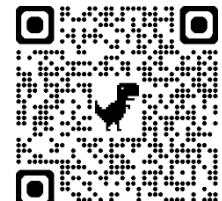
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



QR 4: Recht am
eigenen Bild

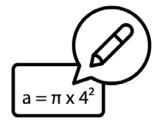


QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"



Weitere Quellen:

- BigData-Insider:
<https://www.bigdata-insider.de/allzeit-zu-diensten-big-data-und-das-smarte-zuhause-a-fbd3d32a4f99b74218477e0729ee398b/>
- Draeger-it:
<https://draeger-it.blog/smart-home-und-data-science-die-verbinding-zwischen-technologie-und-daten/>
- Data&Privacy:
<https://www.dataandprivacy.de/Smart-Home-und-die-DSGVO-ceng.html>
- Haustec.de:
<https://www.haustec.de/gebaeudehuelle/gebaeudeautomation/datschutz-im-smarthome-so-sichern-sie-persoennliche-daten>



1. Podcast-Interviewer-Leitfaden (5-Minuten Podcast)

Frage 1:

Was sind Smart Homes und welche Daten sammeln sie?

Ziel: Einführung in die Welt der vernetzten Haushalte und welche Arten von Daten (z.B. Energieverbrauch, Nutzungsgewohnheiten, Sicherheitsdaten) durch smarte Geräte erfasst werden.

Frage 2:

Wie nutzen Unternehmen und Drittanbieter die gesammelten Daten aus Smart Homes?

Ziel: Erklärung der Verwendung der Daten für Serviceverbesserungen, personalisierte Angebote und die Optimierung von Energie- oder Sicherheitsdiensten.

Frage 3:

Welche Auswirkungen hat die Datennutzung durch Unternehmen auf die Bewohner von Smart Homes? Ist das fair?

Ziel: Diskussion über die Vor- und Nachteile von personalisierten Diensten, Datenschutzbedenken und mögliche Diskriminierung oder Nachteile durch umfassende Datenüberwachung im Haushalt.

Frage 4:

Welche Risiken bestehen generell für die Privatsphäre der Bewohner durch die Datensammlung in Smart Homes?

Ziel: Vertiefung der Datenschutzthemen, einschließlich Datenmissbrauch, Weitergabe an Dritte, und das Risiko von Hackerangriffen auf vernetzte Geräte.

Frage 5:

Wie schützt die DSGVO die Nutzer von Smart Homes, und welche Rechte haben sie in Bezug auf ihre Daten?

Ziel: Erläuterung der relevanten DSGVO-Artikel, z.B. Recht auf Auskunft, Recht auf Löschung, und wie diese im Kontext von Smart-Home-Geräten und -Daten angewendet werden.

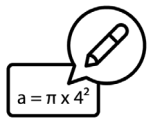
Frage 6:

Welche Maßnahmen können Bewohner ergreifen, um ihre Daten zu schützen und sicherzustellen, dass ihre Privatsphäre gewahrt bleibt, insbesondere im Hinblick auf vernetzte Geräte im Smart Home?

Ziel: Praktische Tipps und Empfehlungen, wie Nutzer Datenschutzeinstellungen anpassen, Einwilligungen verwalten und bewusst mit Smart-Home-Diensten umgehen können.



SMART HOME UND IOT



Smart Home und IoT – wer hört alles zu?

Smart Home und das Internet der Dinge (IoT) – Vernetzte Haushalte, Big Data und Datenschutz

Das Konzept des Smart Homes beschreibt ein Zuhause, in dem verschiedene Geräte und Systeme über das Internet miteinander verbunden sind und automatisch oder per Fernsteuerung bedient werden können. Dazu gehören smarte Thermostate, Beleuchtungssysteme, Überwachungskameras, intelligente Lautsprecher und Haushaltsgeräte wie Kühlschränke und Waschmaschinen. Durch die Nutzung von Sensoren und Vernetzung ermöglichen Smart Homes eine verbesserte Kontrolle und Effizienz im Alltag. **Big Data** spielt auch hier eine entscheidende Rolle. Die in einem Smart Home generierten Daten bieten Einblicke in das Nutzerverhalten, zum Beispiel in Bezug auf Energieverbrauch, Gewohnheiten oder Sicherheitsbedürfnisse. Unternehmen können diese Daten nutzen, um ihre Produkte zu verbessern oder gezielte Dienstleistungen anzubieten. Besonders relevant sind dabei auch personalisierte Dienste, die auf den individuellen Vorlieben der Nutzer basieren. Ein Beispiel für die Nutzung von Daten in Smart Homes ist der Energiemarkt. Intelligente Stromzähler (Smart Meter) sammeln Daten über den Energieverbrauch und ermöglichen es, den Energieeinsatz effizienter zu gestalten oder Tarife dynamisch anzupassen. Allerdings bedeutet dies auch, dass Energieversorger detaillierte Informationen über den Alltag ihrer Kunden erhalten. Diese Entwicklungen werfen Fragen hinsichtlich des Datenschutzes auf. Geräte, die ständig Daten über unsere Aktivitäten sammeln, bergen das Risiko von Missbrauch oder unerlaubtem Zugriff. Zudem könnten sensible Informationen ohne ausreichende Einwilligung an Dritte weitergegeben oder für andere Zwecke verwendet werden. Die **Datenschutz-Grundverordnung (DSGVO)** der EU ist auch hier relevant und sichert den Schutz personenbezogener Daten. Nutzer haben das Recht zu wissen, welche Daten gesammelt werden, und können verlangen, dass diese gelöscht oder nicht mehr verwendet werden.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind Smart Homes und welche Daten sammeln sie?
- Wie nutzen Unternehmen und Drittanbieter die gesammelten Daten aus Smart Homes?
- Welche Auswirkungen hat die Datennutzung durch Unternehmen auf die Bewohner von Smart Homes? Ist das fair?
- Welche Risiken bestehen für die Privatsphäre der Bewohner durch die Datensammlung in Smart Homes?
- Wie schützt die DSGVO die Nutzer von Smart Homes, und welche Rechte haben sie in Bezug auf ihre Daten?
- Welche Maßnahmen können Nutzer ergreifen, um ihre Daten in einem Smart Home zu schützen?

Aufgabe 2: Erstelle ein 2-Minuten-Video zu dem Thema, das alles Relevante zu dem Thema erklärt und die rechtliche Lage einbezieht. Ein Szenen-Beispiel findest du auf der Rückseite. Du kannst auch eigene Ideen einbringen. Nutze iMovie/Clips zum Erstellen und Bearbeiten der Inhalte.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



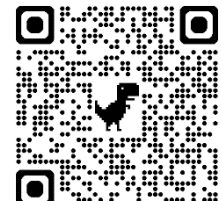
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



QR 4: Recht am
eigenen Bild



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

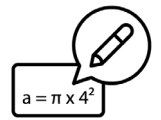


Weitere Quellen:

- BigData-Insider:
<https://www.bigdata-insider.de/allzeit-zu-diensten-big-data-und-das-smarte-zuhause-a-fbd3d32a4f99b74218477e0729ee398b/>
- Draeger-it:
<https://draeger-it.blog/smart-home-und-data-science-die-verbinding-zwischen-technologie-und-daten/>
- Data&Privacy:
<https://www.dataandprivacy.de/Smart-Home-und-die-DSGVO-ceng.html>
- Haustec.de:
<https://www.haustec.de/gebaeudehuelle/gebaeudeautomation/datschutz-im-smarthome-so-sichern-sie-persoенliche-daten>



SMART HOME UND IOT



Titel: „Dein Smart Home, deine Daten – Wer schaut mit?“

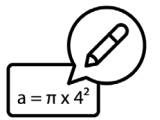
Ort: Ein modernes Wohnzimmer mit verschiedenen Smart-Home-Geräten. Person A sitzt auf dem Sofa und spricht mit Person B.

Dialog:

- **Person A (freudig):** „Schau mal, mein Smart Home ist so praktisch! Ich kann alles mit meinem Handy steuern, sogar, wenn ich nicht zu Hause bin.“
- **Person B (nachdenklich):** „Klingt super, aber weißt du, welche Daten all diese Geräte sammeln?“
- **Person A (überrascht):** „Ähm, naja, hauptsächlich, wie viel Strom ich verbrauche und wann ich die Geräte benutze, oder?“
- **Person B (ernst):** „Es geht um viel mehr. Deine Geräte wissen, wann du zu Hause bist, wie oft du Licht anmachst und sogar, was du in deinem Kühlschrank hast.“
- **Person A (besorgt):** „Wow, das klingt invasiv. Was passiert, wenn diese Daten missbraucht werden?“
- **Person B (erklärend):** „Genau das ist das Problem. Diese Informationen könnten an Werbeanbieter oder sogar an Sicherheitsdienste weitergegeben werden. Du musst sicherstellen, dass du weißt, was mit deinen Daten passiert.“
- **Person A (entschlossen):** „Okay, das sollte ich wirklich genauer prüfen. Wie kann ich sicherstellen, dass meine Daten geschützt bleiben?“

Schlusszene:

Text auf dem Bildschirm: „Bleib informiert und schütze deine Daten in deinem Smart Home. #DSGVO #SmartHome #Datenschutz #IoT“



Smart Home und IoT – wer hört alles zu?

Smart Home und das Internet der Dinge (IoT) – Vernetzte Haushalte, Big Data und Datenschutz

Das Konzept des Smart Homes beschreibt ein Zuhause, in dem verschiedene Geräte und Systeme über das Internet miteinander verbunden sind und automatisch oder per Fernsteuerung bedient werden können. Dazu gehören smarte Thermostate, Beleuchtungssysteme, Überwachungskameras, intelligente Lautsprecher und Haushaltsgeräte wie Kühlschränke und Waschmaschinen. Durch die Nutzung von Sensoren und Vernetzung ermöglichen Smart Homes eine verbesserte Kontrolle und Effizienz im Alltag. **Big Data** spielt auch hier eine entscheidende Rolle. Die in einem Smart Home generierten Daten bieten Einblicke in das Nutzerverhalten, zum Beispiel in Bezug auf Energieverbrauch, Gewohnheiten oder Sicherheitsbedürfnisse. Unternehmen können diese Daten nutzen, um ihre Produkte zu verbessern oder gezielte Dienstleistungen anzubieten. Besonders relevant sind dabei auch personalisierte Dienste, die auf den individuellen Vorlieben der Nutzer basieren. Ein Beispiel für die Nutzung von Daten in Smart Homes ist der Energiemarkt. Intelligente Stromzähler (Smart Meter) sammeln Daten über den Energieverbrauch und ermöglichen es, den Energieeinsatz effizienter zu gestalten oder Tarife dynamisch anzupassen. Allerdings bedeutet dies auch, dass Energieversorger detaillierte Informationen über den Alltag ihrer Kunden erhalten. Diese Entwicklungen werfen Fragen hinsichtlich des Datenschutzes auf. Geräte, die ständig Daten über unsere Aktivitäten sammeln, bergen das Risiko von Missbrauch oder unerlaubtem Zugriff. Zudem könnten sensible Informationen ohne ausreichende Einwilligung an Dritte weitergegeben oder für andere Zwecke verwendet werden. Die **Datenschutz-Grundverordnung (DSGVO)** der EU ist auch hier relevant und sichert den Schutz personenbezogener Daten. Nutzer haben das Recht zu wissen, welche Daten gesammelt werden, und können verlangen, dass diese gelöscht oder nicht mehr verwendet werden.



Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind Smart Homes und welche Daten sammeln sie?
- Wie nutzen Unternehmen und Drittanbieter die gesammelten Daten aus Smart Homes?
- Welche Auswirkungen hat die Datennutzung durch Unternehmen auf die Bewohner von Smart Homes? Ist das fair?
- Welche Risiken bestehen für die Privatsphäre der Bewohner durch die Datensammlung in Smart Homes?
- Wie schützt die DSGVO die Nutzer von Smart Homes, und welche Rechte haben sie in Bezug auf ihre Daten?
- Welche Maßnahmen können Nutzer ergreifen, um ihre Daten in einem Smart Home zu schützen?

Aufgabe 2: Gestalte einen „Schon gewusst?“-Flyer zu dem Thema. Einen Grobentwurf kannst du auf der Rückseite entdecken. Bringe auch eigene Ideen und Gestaltungen ein. Nutze Freeform oder SketchesSchool zum Entwerfen des Flyers.



QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



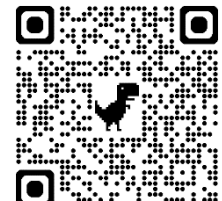
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



QR 4: Recht am
eigenen Bild



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

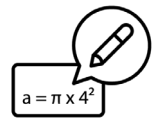


Weitere Quellen:

- BigData-Insider:
<https://www.bigdata-insider.de/allzeit-zu-diensten-big-data-und-das-smarte-zuhause-a-fbd3d32a4f99b74218477e0729ee398b/>
- Draeger-it:
<https://draeger-it.blog/smart-home-und-data-science-die-verbinding-zwischen-technologie-und-daten/>
- Data&Privacy:
<https://www.dataandprivacy.de/Smart-Home-und-die-DSGVO-ceng.html>
- Haustec.de:
<https://www.haustec.de/gebaeudehuelle/gebaeudeautomation/datschutz-im-smarthome-so-sichern-sie-persoенliche-daten>



SMART HOME UND IOT



Flyer-Inhalt: „Schon gewusst?“ – Smart Home und Datenschutz (KI generiert)

1. Überschrift:

- **Position:** Oben, zentriert.
- **Text:** „Schon gewusst?“ in großer, fetter Schrift.
- **Schriftart:** Moderne, klare Schriftart (z.B. Arial oder Helvetica).
- **Farbe:** Blau, um Aufmerksamkeit zu erregen.

2. Einleitender Text:

- **Position:** Direkt unter der Überschrift.
- **Text:** Smart Homes machen unseren Alltag einfacher, indem sie Geräte miteinander vernetzen und automatisieren. Doch gleichzeitig sammeln diese Systeme kontinuierlich Daten über unser Verhalten, unseren Energieverbrauch und sogar unsere Sicherheitsbedürfnisse. Diese Daten können missbraucht oder ohne unser Wissen an Dritte weitergegeben werden.
- **Schriftart:** Kleinere, gut lesbare Schrift.
- **Farbe:** Schwarz oder dunkles Grau.

3. Fakten und Tipps:

- **Position:** In der Mitte, als Liste angeordnet.
- **Text:** 3–4 Tipps, z.B.:
 - „Überprüfe regelmäßig die Datenschutzeinstellungen deiner Smart-Home-Geräte.“
 - „Achte darauf, welche Daten du freigibst und an wen.“
 - „Lies die Datenschutzerklärungen, bevor du neue Geräte installierst.“
 - „Nutze dein Recht auf Auskunft und Löschung gemäß DSGVO.“
- **Schriftart:** Leicht hervorgehoben (z.B. fett oder kursiv), damit die Tipps ins Auge fallen.
- **Farbe:** Schwarz für den Text, Blau für Aufzählungspunkte oder Nummern, um die Liste hervorzuheben.

4. Grafik/Symbol:

- **Position:** Unten rechts.
- **Bild:** Ein Symbol eines vernetzten Hauses mit einem Datenschuttschild oder Schloss.
- **Größe:** Dezent und klein, um den Text zu unterstreichen.

5. Abschlusssatz:

- **Position:** Unten links, neben der Grafik.
- **Text:** „Bleib informiert und schütze deine Daten zu Hause. #DSGVO #SmartHome #IoT #Datenschutz.“
- **Schriftart:** Klein, aber gut lesbar.
- **Farbe:** Blau oder Grau, um sich harmonisch in das Design einzufügen.

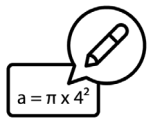
Gestaltungstipps:

- **Weißer Raum:** Nutze weißen Raum, um den Flyer nicht zu überladen und die Lesbarkeit zu erhöhen.
- **Symmetrie:** Eine symmetrische Anordnung hilft, das Design sauber und professionell wirken zu lassen.
- **Farbharmonie:** Verwende eine konsistente Farbpalette (Blau und Grau), um ein harmonisches Erscheinungsbild zu erzielen.
- **Klare Schriftarten:** Wähle gut lesbare Schriftarten für alle Textelemente, um die Verständlichkeit zu gewährleisten.





SMART HOME UND IOT



Smart Home und IoT – wer hört alles zu?

Smart Home und das Internet der Dinge (IoT) – Vernetzte Haushalte, Big Data und Datenschutz

Das Konzept des Smart Homes beschreibt ein Zuhause, in dem verschiedene Geräte und Systeme über das Internet miteinander verbunden sind und automatisch oder per Fernsteuerung bedient werden können. Dazu gehören smarte Thermostate, Beleuchtungssysteme, Überwachungskameras, intelligente Lautsprecher und Haushaltsgeräte wie Kühlschränke und Waschmaschinen. Durch die Nutzung von Sensoren und Vernetzung ermöglichen Smart Homes eine verbesserte Kontrolle und Effizienz im Alltag. **Big Data** spielt auch hier eine entscheidende Rolle. Die in einem Smart Home generierten Daten bieten Einblicke in das Nutzerverhalten, zum Beispiel in Bezug auf Energieverbrauch, Gewohnheiten oder Sicherheitsbedürfnisse. Unternehmen können diese Daten nutzen, um ihre Produkte zu verbessern oder gezielte Dienstleistungen anzubieten. Besonders relevant sind dabei auch personalisierte Dienste, die auf den individuellen Vorlieben der Nutzer basieren. Ein Beispiel für die Nutzung von Daten in Smart Homes ist der Energiemarkt. Intelligente Stromzähler (Smart Meter) sammeln Daten über den Energieverbrauch und ermöglichen es, den Energieeinsatz effizienter zu gestalten oder Tarife dynamisch anzupassen. Allerdings bedeutet dies auch, dass Energieversorger detaillierte Informationen über den Alltag ihrer Kunden erhalten. Diese Entwicklungen werfen Fragen hinsichtlich des Datenschutzes auf. Geräte, die ständig Daten über unsere Aktivitäten sammeln, bergen das Risiko von Missbrauch oder unerlaubtem Zugriff. Zudem könnten sensible Informationen ohne ausreichende Einwilligung an Dritte weitergegeben oder für andere Zwecke verwendet werden. Die **Datenschutz-Grundverordnung (DSGVO)** der EU ist auch hier relevant und sichert den Schutz personenbezogener Daten. Nutzer haben das Recht zu wissen, welche Daten gesammelt werden, und können verlangen, dass diese gelöscht oder nicht mehr verwendet werden.

Aufgabe 1: Nutzungsrechte, Recht am eigenen Bild, Recht auf Vergessenwerden, DSGVO und Privatsphäre

- Was sind Smart Homes und welche Daten sammeln sie?
- Wie nutzen Unternehmen und Drittanbieter die gesammelten Daten aus Smart Homes?
- Welche Auswirkungen hat die Datennutzung durch Unternehmen auf die Bewohner von Smart Homes? Ist das fair?
- Welche Risiken bestehen für die Privatsphäre der Bewohner durch die Datensammlung in Smart Homes?
- Wie schützt die DSGVO die Nutzer von Smart Homes, und welche Rechte haben sie in Bezug auf ihre Daten?
- Welche Maßnahmen können Nutzer ergreifen, um ihre Daten in einem Smart Home zu schützen?

Aufgabe 2: Erstelle eine Social-Media-Kampagne auf Instagram zu diesem Thema. Die Kampagne soll den 5-Minuten-Podcast, den 2-Minuten-Clip und den Aufklärungsflyer der anderen Gruppen beinhalten. Dabei sollst du auch mögliche Posts/Stories erstellen, die man auf einem neuen Profil posten könnte. Auf der Rückseite findest du eine Beispiel-Kampagne.



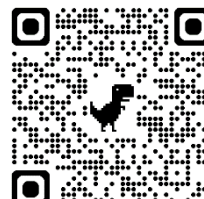
QR 1: DSGVO Art. 17
"Recht auf
Vergessenwerden"



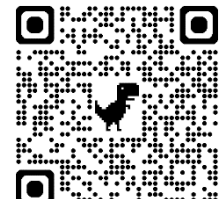
QR 2: DSGVO Art. 9
Verarbeitung
personenbezogener
Daten



QR 3: DSGVO Artikel
12 bis 22 z.B. Recht
auf Auskunft, Recht
auf Berechtigung,
Recht auf
Widerspruch



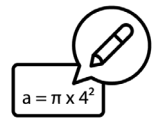
QR 4: Recht am
eigenen Bild



QR 5: DSGVO Art. 6
"Rechtmäßigkeit
der Verarbeitung"

Weitere Quellen:

- BigData-Insider:
<https://www.bigdata-insider.de/allzeit-zu-diensten-big-data-und-das-smarte-zuhause-a-fbd3d32a4f99b74218477e0729ee398b/>
- Draeger-it:
<https://draeger-it.blog/smart-home-und-data-science-die-verbinding-zwischen-technologie-und-daten/>
- Data&Privacy:
<https://www.dataandprivacy.de/Smart-Home-und-die-DSGVO-ceng.html>
- Haustec.de:
<https://www.haustec.de/gebaeudehuelle/gebaeudeautomation/datschutz-im-smarthome-so-sichern-sie-persoенliche-daten>



Social-Media-Kampagne: Smart Home, IoT und Datenschutz

Beitrag 1: Podcast-Ankündigung

- **Bild/Video:** Ein animiertes Bild mit dem Titel „Smart Home und Datenschutz: Was du wissen musst“ und einem Play-Button.
- **Text (Post-Beschreibung):** „🎧 Dein Zuhause ist vernetzt, aber wer hat Zugriff auf deine Daten? Erfahre in unserem neuen Podcast, wie Smart Homes und IoT funktionieren und was das für deine Privatsphäre bedeutet. 📶 Hör jetzt rein! #SmartHome #IoT #BigData #Datenschutz #DSGVO“

Beitrag 2: 2-Minuten-Video „Dein Zuhause, deine Daten“

- **Bild/Video:** Ein 2-minütiges Video, das eine Unterhaltung über die Datensammlung in Smart Homes und deren Nutzung durch Unternehmen zeigt.
- **Text (Post-Beschreibung):** „👁️ Deine Smart-Home-Geräte sammeln Daten über dich! In unserem neuen Video erfährst du, wie Unternehmen diese Daten nutzen und was du tun kannst, um deine Privatsphäre zu schützen. #SmartHome #IoT #BigData #Datenschutz #DSGVO“

Beitrag 3: Aufklärungsflyer

- **Bild:** Der Flyer über Smart Home, IoT und Datenschutz.
- **Text (Post-Beschreibung):**

„📄 Lade unseren Flyer herunter und erfahre, wie du deine Daten in deinem vernetzten Zuhause schützen und bewusst mit Smart-Home-Geräten umgehen kannst!“

#Flyer #SmartHome #IoT #Datenschutz #BigData #DSGVO“

Zusätzliche Post-Ideen:

Post-Idee 1: Quiz zu Daten und Smart Homes

- **Bild:** Ein interaktives Bild mit der Quiz-Frage: „Weißt du, welche Daten deine Smart-Home-Geräte von dir sammeln?“ mit Antwortmöglichkeiten wie: „Ja, voll im Bilde!“ oder „Nein, erzähl mir mehr!“
- **Text:** „Teste dein Wissen! Weißt du, welche Daten durch Smart-Home-Geräte gesammelt werden und was das für dich bedeutet? Nimm an unserem Quiz teil und finde es heraus! #SmartHome #IoT #Quiz #Datenschutz #DSGVO“

Post-Idee 2: Fakten über Smart Homes, IoT und Datenschutz

- **Bild:** Eine Infografik mit Fakten zu Smart Homes, z.B.: „Wusstest du, dass deine Smart-Home-Geräte rund um die Uhr Daten sammeln? Lerne, wie du deine Daten schützt!“
- **Text:** „Schon gewusst? Unternehmen nutzen Daten aus Smart Homes, um personalisierte Angebote zu erstellen. Erfahre, wie du die Kontrolle behältst und deine Privatsphäre schützt! #SmartHome #IoT #Datensicherheit #BigData #DSGVO“

Story-Idee: Umfrage zu Smart Homes und Privatsphäre

- **Frage:** „Hast du Smart-Home-Geräte in deinem Zuhause? Weißt du, welche Daten dabei gesammelt werden?“
- **Optionen:** „Ja, und ich bin informiert!“ / „Nein, keine Ahnung!“
- **Ergebnis:** Bei „Nein“ könnte ein Swipe-up-Link zu einem erklärenden Video oder einem Infopost geleitet werden.

Post-Idee 3: Tutorial zum Schutz deiner Daten im Smart Home

- **Bild:** Ein Bild eines Hauses mit einem Schloss oder Datenschutzsymbol und verschiedenen Smart-Home-Geräten.
- **Text:** „Deine Daten sind wertvoll – auch in deinem Zuhause. Erfahre in unserem Tutorial, wie du verantwortungsbewusst mit Smart-Home-Geräten umgehst und deine Privatsphäre schützt! #SmartHome #IoT #Datenschutz #DSGVO #SicherZuhause“