



**Titel:**

Datenschutz – leicht erklärt  
Arbeitsblattsammlung zur gleichnamigen Videoreihe der Initiative „Datenschutz geht zur Schule“

**Autorin:**

Stefanie Rack, EU-Initiative klicksafe

**Herausgeber:**

Initiative „Datenschutz geht zur Schule“ des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. und der privacy4people – Gesellschaft zur Förderung des Datenschutzes gGmbH (P4P gGmbH) (beide Budapester Str. 31, 10787 Berlin) in Zusammenarbeit mit der EU-Initiative klicksafe und mit Unterstützung der DATEV-Stiftung Zukunft.

Die 2009 vom BvD gegründete und seit 2020 von dessen gemeinnütziger Gesellschaft P4P gGmbH fortgeführte Initiative „Datenschutz geht zur Schule“ zeigt Schüler\*innen einfache Wege auf, wie sie ihre persönlichen Daten besser schützen können – ohne dabei auf moderne Kommunikationsformen verzichten zu müssen.

1. Auflage Mai 2022

**Projektunterstützung:**

DATEV-Stiftung Zukunft

**Kooperationspartner:**

Die Arbeitsmaterialien in dieser Broschüre wurden gemeinsam mit der EU-Initiative klicksafe [www.klicksafe.de](http://www.klicksafe.de) entwickelt. klicksafe ist das deutsche Awareness Centre im Digital Europe Programm der Europäischen Union und wird gemeinsam von der Medienanstalt Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien NRW in Deutschland umgesetzt.

**Koordinatorinnen klicksafe:**

Birgit Kimmel, Deborah Woldemichael,  
Medienanstalt Rheinland-Pfalz

**Rechtliches**

Die alleinige Verantwortung für diese Veröffentlichung liegt bei den Herausgebern. Es wird darauf verwiesen, dass alle Angaben in diesem Buch trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der Herausgeber und der Autorin ausgeschlossen ist.

Diese Broschüre und die einzelnen Arbeitsblätter stehen unter der Lizenz CC BY NC ND 4.0 und dürfen unter Namensnennung nicht kommerziell und ohne Veränderungen unter Weitergabe gleicher Bedingungen beliebig geteilt werden, d. h. die nichtkommerzielle Nutzung und Verbreitung ist unter Angabe der Quelle „Datenschutz geht zur Schule“, eine Initiative des BvD e.V. und unter Angabe der Webseite [www.dsgzs.de](http://www.dsgzs.de) erlaubt.



<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>

Sollen über die genannte Lizenz hinausgehende Erlaubnisse gewährt werden, können Einzelabsprachen mit der Initiative, vertreten durch die P4P gGmbH getroffen werden. Wenden Sie sich dazu bitte an [kontakt@dsgzs.de](mailto:kontakt@dsgzs.de).

Die Links wurden sorgfältig geprüft. Es kann aber nicht ausgeschlossen werden, dass der Inhalt der Zieladresse geändert wird. Eine Haftung kann daher für die Richtigkeit, Aktualität und Freiheit von Schadsoftware für die verlinkten Seiten nicht übernommen werden. Bitte informieren Sie uns, sollten Sie hierzu Hinweise haben.

**Danksagung:**

Wir danken allen Mitwirkenden, die ihren Beitrag zur Konzeption der Inhalte, Erstellung der Videoclips und dieser Arbeitsblätter leisteten, vor und hinter der Kamera, am Schneidetisch oder im Nachgang bei der Abstimmung zur grafischen Gestaltung bis hin zum Lektorat.

**Layout und Umschlaggestaltung:**

Designgruppe Fanz & Neumayer, Ludwigshafen und Heidelberg

## Vorwort

Die vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. ins Leben gerufene und durch die gemeinnützige P4P gGmbH getragene Initiative „Datenschutz geht zur Schule“ sensibilisiert Schüler\*innen in ganz Deutschland dazu, mit eigenen Daten und den Daten anderer im Internet und in den sozialen Medien sicherer und bewusster umzugehen. Das Sensibilisierungsangebot der ehrenamtlich tätigen Dozent\*innen wurde in den letzten Jahren erfolgreich in den Schulen etabliert.

Um auch in Pandemiezeiten ohne Schulbesuch passende Impulsvorträge liefern zu können, hat die Initiative „Datenschutz geht zur Schule“ mit freundlicher Unterstützung der Datenschutzaufsichtsbehörden LfDI Baden-Württemberg, dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA), dem Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI) sowie dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) im Rahmen des Projektes „Datenschutz – leicht erklärt“ Video-Clips erstellt.

Diese Videos werden jeweils in hoher Qualität oder in Standardqualität (geeignet für die mobile Ansicht) zum Herunterladen angeboten. Sie sind zwischen 1:30 Minuten und knapp 6:00 Minuten lang.

Die insgesamt 18 Einzel-Videos umfassen die wichtigsten Aspekte der Themenspannbreite, die bisher nur in den Klassenräumen im Rahmen der Sensibilisierungsveranstaltungen vermittelt wurden. Die Videos sind in drei Bereiche gegliedert: „Datenschutz“, „technische Themen“ und „naheliegende Themen“ und beinhalten u.a. „Grundlagen zu Datenschutz“, „Meine Rechte im Datenschutz“, Tipps zu „Passworten“, aber auch Hinweise zur Smartphonennutzung oder Besonderheiten bei „Berufsgeheimnisträger\*innen“. Alle Clips ermöglichen auch durch Versionen mit Untertitel einen barrierefreien Einsatz.



<https://www.datenschutz-leicht-erklart.de/>

Um die Nutzung rechtlich möglichst einfach zu gestalten, stehen die Video-Clips unter der Creative Commons Lizenz



<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>

Bei diesen Videos werden Themen angesprochen, zu denen bisher kaum oder wenig Arbeitsblätter für die Nachbearbeitung angeboten werden, so dass zusammen mit Klicksafe versucht wurde diese Lücke zu schließen. Es lassen sich daher hier Arbeitsblätter zu elf der Video-Clips finden, die damit unser Lehrerhandout ergänzen, das weiterhin online auf den Seiten der Initiative „Datenschutz geht zur Schule“ unter <https://www.bvdnet.de/datenschutz-geht-zur-schule/lehrerhandout/> und bei Klicksafe auch in gedruckter Fassung erhältlich ist.

Die Arbeitsblätter hier finden Sie natürlich auch einzeln auf unserer Webseite als pdf.

Ergänzend bieten wir an, dass – vorbehaltlich freier Ressourcen – Sie auch mit unseren Dozent\*innen einen Videokonferenztermin (über Ihr Videokonferenzsystem) im Anschluss an das Betrachten der Videos vereinbaren können, damit diese Folgefragen beantworten. Wenden Sie sich bitte dazu an [kontakt@dsgzs.de](mailto:kontakt@dsgzs.de).

Bei Interesse an Veranstaltungen der Initiative „Datenschutz geht zur Schule“ melden Sie sich bitte unter [kontakt@dsgzs.de](mailto:kontakt@dsgzs.de).

Für Rückmeldungen wie Themenwünsche oder Feedback freuen wir uns über eine Mail an [kontakt@dsgzs.de](mailto:kontakt@dsgzs.de).

All die in den Videos und den Arbeitsblättern steckende Arbeit war nur möglich durch das Engagement aller Beteiligter und die wohlwollende Förderung unserer Initiative durch die DATEV Stiftung Zukunft.

Wenn auch Sie uns unterstützen wollen, ist dies über eine Zuwendung an die P4P gGmbH möglich.

*Rudi Kramer*

Sprecher des AK Schule des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

## Methodisch-didaktische Hinweise – Übersicht über die Projekte

	Arbeitsblatt	Zeit	Kompetenzen
1	Schule und Arbeiten	45 Min.	Die SuS erlangen Sicherheit beim Umgang mit personenbezogenen Daten. Sie erfahren, welche Datenabfragen zulässig und welche unzulässig sind. Sie können Tipps für den Selbstdatenschutz in eigenen Worten formulieren.
2	Selfie	45 Min.	Die SuS lernen Grundsätze des Selbstschutzes bei Formen der Selbstdarstellung im Internet kennen. Sie können Tipps beim Erstellen von Selfies in eigenen Worten formulieren.
3	Webcam	45 Min.	Die SuS können Webcams und Handykameras sicher und datenschutzkonform nutzen.
4	Profiling	45 Min.	Die SuS werden für das Profiling durch Anbieter sozialer Netzwerke sensibilisiert. Sie lernen Schutzmaßnahmen kennen.
5	Smartphone	45 Min.	Die SuS erfahren in einer praktischen Übung, wie sie ihr Smartphone datensparsam und datensicher nutzen können.
6	Passworte	45 Min.	Die SuS verstehen die Wichtigkeit von sicheren Passwörtern. In einer Praxisübung erstellen sie selbst eigene sichere Passwörter.
7	Meine Rechte	45 Min.	Die SuS erfahren, welche Datenschutzrechte man als Verbraucher*in hat. Sie führen ein Auskunftersuchen über die Datenspeicherung in einem selbst gewählten Online-Angebot durch. Sie berichten über ihre Erfahrungen und tauschen sich aus.
8	Internet	45 Min.	Die SuS verstehen die grundlegende Funktionsweise des Internet. Sie können die Vor- und Nachteile von IP-Abfragen erörtern.
9	Schutzmaßnahmen	45 Min.	Die SuS lernen Maßnahmen für den Schutz ihrer Daten kennen. Sie gestalten die Tipps auf einem Informationsposter.
10	IT-Sicherheit	45 Min.	Die SuS lernen Grundlagen der IT-Sicherheit kennen. Sie intensivieren ihr Wissen, indem sie eine Anleitung zu einem der Tipps aus dem Video erstellen.
11	Berufsgeheimnisträger	45 Min.	Die SuS lernen Anforderungen kennen, die sich aus einer berufsrechtlichen Verschwiegenheitspflicht ergeben können.

Material	Zugang Internet /PC	Zielgruppe	
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 6	<b>1</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 6	<b>2</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 6	<b>3</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 6	<b>4</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 6	<b>5</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 6	<b>6</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 8	<b>7</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 8	<b>8</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer; Poster	Ja	Ab Klasse 8	<b>9</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 10	<b>10</b>
Webseite <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer	Ja	Ab Klasse 10	<b>11</b>

# 1 | Datenschutzrechtliche Grundlagen – Schule und Arbeiten

1

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS erlangen Sicherheit beim Umgang mit personenbezogenen Daten. Sie erfahren, welche Datenabfragen zulässig und welche unzulässig sind. Sie können Tipps für den Selbstschutz in eigenen Worten formulieren.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 6

## Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Schule und Arbeiten“ unter → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) auf den eigenen mobilen Geräten oder an einem PC/Tablet an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



### Hintergrund zur Person im Video:

Dr. Mirka Möldner ist Bereichsleiterin am Bayerischen Landesamt für Datenschutzaufsicht (BayLDA). Informationen unter: → [www.lida.bayern.de](http://www.lida.bayern.de)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen zunächst in Stillarbeit. Für Frage 4 ist ein Austausch mit dem\*der Sitznachbar\*in angedacht. Der Austausch sollte im Flüsterton stattfinden.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:

**Aufgabe 2:** Bsp. 1, 2, 4, 5 nicht ok, Bsp. 3 ok

### Aufgabe 3:

- Frage dich selbst, welche Informationen du über dich ans „Schwarze Brett“ deiner Schule hängen würdest.
- Stelle deine Konten auf „privat“, wenn du Inhalte teilst, die privat sind.
- Überlege dir gut, welchen Content anderer du teilst.
- Lehne ungewollte Freundschaftsanfragen ab.
- Erzähle auch im Netz Fremden nicht alles über dich.
- Schau dir die Einstellungen deiner Apps genau an.
- Schütze deine Geräte und Apps mit sicheren Passwörtern (ggf. mit Passwortmanagern).
- Gib deine Passwörter nicht heraus.
- Bleib kritisch.

**Aufgabe 4:** Die eigenen Tipps der SuS können an der Tafel gesammelt und nach Kriterien wie Praktikabilität u.a. sortiert werden.

**Weiterarbeit** Die SuS können Infoposter mit den Sicherheitstipps erstellen und diese in den Klassenräumen der Parallelklassen aufhängen.

## AB 1 | Schule und Arbeiten

### Aufgabe 1:

Schaue dir das Video „Schule und Arbeiten“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.



Dr. Mirka Möldner, Screenshot Erklärvideo

### Aufgabe 2:

Welche Datenabfragen sind aus deiner Sicht ok, welche nicht? Ordne die Beispiele zu, indem du die Nummer des Beispiels in die Tabelle schreibst. Fallen dir selbst weitere Beispiele ein?

*Beispiel 1: Du bist auf der Suche nach einer Ausbildungsstelle. Beim Bewerbungsgespräch fragt dich der Arbeitgeber, ob er Zugang zu deinen Social-Media-Accounts haben kann, damit er mehr über dich erfährt.*

*Beispiel 2: Dein Schwimmtrainer fragt in einem Gruppenchat, in dem alle deine Schwimmkolleg\*innen sind, nach deinen Krankheiten.*

*Beispiel 3: Die Ärztin im Krankenhaus muss für eine anstehende Operation deine Vorerkrankungen und Medikamentenunverträglichkeiten abfragen.*

*Beispiel 4: In einem TikTok-Video fordert ein Influencer alle Zuschauer auf, ihre Telefonnummern in den Chat zu schreiben, damit man sich gegenseitig anrufen kann.*

*Beispiel 5: Ein Mitspieler in einem Onlinespiel will, dass du ihm private Bilder von dir in Unterwäsche schickst.*

ok	Nicht ok

### Aufgabe 3:

Welche Tipps werden im Video gegeben? Notiere in eigene Worten!

---



---



---



---

### Aufgabe 4:

Füge mindestens einen eigenen Tipp hinzu und tausche dich im Flüsterton mit deinem\*deiner Sitznachbar\*in aus.

## 2 | Datenschutzrechtliche Grundlagen – Selfie

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS lernen Grundsätze des Selbstschutzes bei Formen der Selbstdarstellung im Internet kennen. Sie können Tipps beim Erstellen von Selfies in eigenen Worten formulieren.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 6

### Verlaufsplanung

**Einstieg** Die SuS schauen sich das Erklärvideo „Selfie“ unter → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) auf den eigenen mobilen Geräten oder an einem PC/Tablet an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.

**i Hintergrund zur Person im Video:**  
Melanie Schoch ist Dozentin der Initiative „Datenschutz geht zur Schule“.  
Informationen unter: → [www.bvdnet.de/datenschutz-geht-zur-schule/](http://www.bvdnet.de/datenschutz-geht-zur-schule/)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus.  
Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:

**Aufgabe 2:** „Jeder, der ein Bild böse verändert, und dann damit beispielsweise einen anderen mobben möchte, der befindet sich im Straftatbestand. Mobbing ist eine Straftat und hat auch im Netz nichts zu suchen.“  
Fragen Sie die SuS in einem anschließenden Gespräch nach möglichen weiteren Folgen von Bildermisbrauch, wie bspw. beim Cyber-Grooming. Falls SuS von Erlebnissen in ihrem Umfeld berichten wollen, achten Sie darauf, dass allgemein und neutral formuliert wird, damit keine privaten Details öffentlich werden → Aspekt Daten- und Persönlichkeitsschutz!

**Aufgabe 3:**  
Definition: Recht am eigenen Bild  
Das Recht am eigenen Bild ist als besondere Ausprägung des allgemeinen Persönlichkeitsrechts im Kunsturhebergesetz (KunstUrhG) definiert. Gem. § 22 Satz 1 KunstUrhG dürfen Abbildungen einer (erkennbaren) Person grundsätzlich nur dann verbreitet oder zur Schau gestellt werden, wenn deren Einwilligung vorliegt. Es gibt Ausnahmen z.B. für Versammlungen, prominente Personen, wenn man auf der Aufnahme nur Beiwerk ist oder wenn es um künstlerische Werke geht.

**Aufgabe 4:**

1. Achtet auf eure Bildrechte und die Rechte anderer.
2. Achtet auf Gesetze die Privatsphäre betreffen, vor allem, wenn andere abgebildet sein sollen.
3. Achtet auf Gesetze, die das Persönlichkeitsrecht der abgebildeten Person betreffen.
4. Echtheit: Denkt an die Echtheit im Bild, setzt auf Natürlichkeit, zeigt euch wie ihr seid!
5. Fairness: Mobbing hat im Netz nichts zu suchen! Manipuliert die Bilder nicht nachteilig und verletzt keine anderen.
6. Be your Selfie: Verteilt nur Bilder hinter denen ihr stehen könnt, denn Löschen ist unmöglich!

Die SuS können noch weitere Tipps ergänzen, die in der Klasse besprochen werden. Sammeln Sie außerdem gemeinsam Beispiele aus dem alltäglichen Leben für die Tipps 1–6.

Beispiele

**Tip 2:** Keine Fotos in höchstpersönlichem Lebensbereich wie fremder Wohnung, Umkleidekabine etc.

**Tip 3:** Auch im privaten Bereich sind Persönlichkeitsrechte anderer Personen zu beachten. Beispiel: SuS treffen lokalen Sportstar in ihrem Lieblingscafé: sie dürfen ihn fotografieren, aber z. B. nicht, wenn er seine\*n Freund\*in küsst. Sobald Bilder mit Personen ins Internet hochgeladen werden, und damit öffentlich zugänglich sind, verlässt man dabei den privaten/familiären Bereich und braucht eine datenschutzrechtliche Grundlage, wie z.B. die Einwilligung der abgebildeten Personen.

**Weiterarbeit****a) Flyer und Unterrichtsmaterial zum Thema Bildrechte**

Welche Regeln sollten gelten, wenn man Fotos über Messenger Apps oder soziale Netzwerke öffentlich teilt? Wie gehen die SuS selbst mit ihren Fotos im Internet um? Das Unterrichtsmaterial und der Flyer „Zu nackt fürs Internet?“ hilft den SuS in 10 Schritten beim souveränen Umgang mit Fotos im Internet.

Link: Unterrichtseinheit

→ [www.klicksafe.de/materialien/zu-nackt-fuers-internet-begleitmaterial-zum-klicksafe-flyer/](http://www.klicksafe.de/materialien/zu-nackt-fuers-internet-begleitmaterial-zum-klicksafe-flyer/)

Link Flyer:

→ [www.klicksafe.de/materialien/zu-nackt-fuers-internet-fuer-jugendliche/](http://www.klicksafe.de/materialien/zu-nackt-fuers-internet-fuer-jugendliche/)

**b) Kreatives Schreiben**

Hausaufgabe:

„Wenn ihr ein Bild (im Internet) verteilt, verliert ihr jede Kontrolle über dieses Bild“ (Zitat aus dem Video). Schreibt eine Kurzgeschichte (max. 2 Seiten) zu dieser Aussage.

## AB 2 | Selfie

### Aufgabe 1:

Schaue dir das Video „Selfie“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Ergänze die fehlenden Wörter aus dem Video  
in dem Satz:

„Jeder, der ein ..... böseartig  
verändert, und dann damit beispielsweise  
einen anderen mobben möchte, der befindet  
sich im .....

Mobbing ist eine ..... und hat auch im Netz nichts zu suchen.“

Der Missbrauch von Bildern hat häufig besonders schlimme Folgen. Sprecht darüber in der Klasse.

### Aufgabe 3:

Was ist eigentlich das Recht am eigenen Bild? Recherchiert im Internet und schreibt die Definition in den leeren Infokasten.

**Definition „Recht am eigenen Bild“:**

### Aufgabe 4:

Schaut euch das Video noch einmal an. Notiert die 6 Tipps aus der Zusammenfassung im Video  
in eigenen Worten:

---

---

---

---

---

---



### 3 | Datenschutzrechtliche Grundlagen – Webcam

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS können Webcams und Handykameras sicher und datenschutzkonform nutzen.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 6

#### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Webcam“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



#### Hintergrund zur Person im Video:

Katarina Leikert ist Dozentin der Initiative „Datenschutz geht zur Schule“. Informationen unter: → [www.bvdnet.de/datenschutz-geht-zur-schule/](http://www.bvdnet.de/datenschutz-geht-zur-schule/)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:

#### Aufgabe 2:

1. Systemeinstellungen am Smartphone: Verwendung der Kamera für jede App aktiv zustimmen.
2. Bei Verwendung der Kamera: Hintergrundfilter einrichten, um andere im Raum zu schützen.
3. Bei Nichtverwendung: Kamera abkleben.

#### Aufgabe 3:

Die SuS suchen sich eine der beiden Aufgaben aus und erstellen eine Anleitung, in der sie beschreiben, wo genau die Funktionen gefunden werden können. Die Anleitungen können im Plenum verglichen werden. Die SuS verteilen die Anleitung an eine ihnen nahestehende Person und betreiben damit selbst Aufklärungsarbeit.

Als Beispiel kann das Bild im Anhang präsentiert werden. Es zeigt die Systemeinstellungen „Kamera aus“ für ein iPhone Version 14.7.1 und die App WhatsApp.

**Weiterarbeit** Keine Chance für Webcam-Spione! Die SuS basteln ein Webcam-Cover. Anleitungen finden sich auf YouTube wie bspw. unter: → <https://ogy.de/00hx>.

## AB 3 | Webcam (1/2)

### Aufgabe 1:

Schaue dir das Video „Webcam“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Webcams und auch Handykameras sind große  
Schwachstellen in unseren Geräten.  
Welche **3 Tipps zum Schutz** gibt Katarina Leikert  
im Video?



---

---

---

---

### Aufgabe 3:

Übung: Suche dir eine der beiden Aufgaben aus und finde heraus, wie du die Einstellung an deinem Gerät machen kannst.

- a) Wie stellst du die Kamera für einzelne Apps bei dir am Smartphone aus?
- b) Wie stellst du den Hintergrundfilter ein bei deinem Videokonferenz-Programm?

Schreibe eine Anleitung und gib sie einer Person, die sie auch gebrauchen kann, bspw. deinen Eltern, Geschwistern, Großeltern.

---

---

---

---

---

---

---

---

### AB 3 | Webcam (2/2)



3

Abbildung Screenshot iOS 14.7.1. Systemeinstellungen WhatsApp

## 4 | Datenschutzrechtliche Grundlagen – Profiling

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS werden für das Profiling durch Anbieter sozialer Netzwerke sensibilisiert. Sie lernen Schutzmaßnahmen kennen.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 6

### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Profiling“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



#### Hintergrund zur Person im Video:

Enya ist Schülerin einer 7. Klasse. Dirk Wolf ist Dozent der Initiative „Datenschutz geht zur Schule“.

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Arbeitsergebnisse der Aufgaben 2 und 3 im Plenum. Bei Aufgabe 3 können Situationen genannt werden, in denen Personen durch ihre öffentlichen Angaben im Internet ausspioniert werden. Die Folgen reichen von Überfällen oder Einbrüchen bis hin zu Erpressung (aufgrund geposteter Bilder oder Informationen wie bspw. bei Sexting), oder auch gezielte (unerwünschte) Werbung und Prognosen über Bedürfnisse oder Vermögensverhältnisse.

**Weiterarbeit** Als Hausaufgabe könnte ein kreativer Schreibauftrag zum Thema „Tägliche Datenspuren“ erfolgen. Eine Sammlung herausragender Einreichungen beim Datenschutz Medienpreis des BvD aus den letzten Jahren, die sich auch für den Einsatz im Unterricht anbieten, finden Sie hier: → [www.bvdnet.de/rueckblick-datenschutz-medienpreis-2019](http://www.bvdnet.de/rueckblick-datenschutz-medienpreis-2019)



Für ältere SuS: Datenexperiment: „Made to measure“ (Einreichung DAME 2021)  
 Das Künstlerkollektiv Laokoon hat auf Grundlage der Google Suchen einer Person versucht diese Person und ihr Leben nachzubilden und damit einen digitalen Doppelgänger erstellt. Das Projekt-Video finden Sie unter: → [www.madetomeasure.online](http://www.madetomeasure.online)

## AB 4 | Profiling (1/2)

### Aufgabe 1:

Schaue dir das Video „Profiling“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

„Auf Instagram, Snapchat, TikTok und Co. kannst du einstellen, wer deine Posts sehen kann. Denn über Posts lernt das Internet viel über dich und erstellt sogenannte Profile. Zum Beispiel sagt schon viel über dich aus, was du gerne isst oder was du gerne trinkst. Mit genauen Profilen kann dir Werbung ausgespielt werden.“



Enya, Screenshot Erklärvideo

Daten über dich zu sammeln, diese auszuwerten und Profile über dich zu erstellen nennt man Profiling! Dazu gehören u.a. deine Interessen, dein Verhalten und deine Eigenschaften. Stell dir vor, du bist für die Werbung in einem sozialen Netzwerk zuständig. Erstelle ein kurzes Profil über die Personen, die solche Bilder posten. Welche Werbung würdest du ihnen anzeigen?

	 <p>Quelle: <a href="http://www.flickr.com/verchmarco">www.flickr.com/verchmarco</a></p>	 <p>Quelle: <a href="https://pixabay.com/amiraxgelcola">https://pixabay.com/amiraxgelcola</a></p>	 <p>Quelle: Howief, CC BY-SA 3.0 &lt;<a href="https://creativecommons.org/licenses/by-sa/3.0/">https://creativecommons.org/licenses/by-sa/3.0/</a>&gt;, via Wikimedia Commons</p>
Profil der Person:			
Werbung:			

### Aufgabe 3:

„Es können aber auch Menschen auf dich aufmerksam werden, die dir nichts Gutes wollen.“ sagt Enya im Video. Was meint sie damit? Tausche dich mit deinem\*deiner Sitznachbar\*in aus.

## AB 4 | Profiling (2/2)

### Zusatzaufgabe/Hausaufgabe:

Welche Datenspuren hinterlässt du im Internet an einem Tag?

Notiere einen Tag lang, welche Medien du morgens, mittags und abends nutzt. Unterstreiche die Situationen, in denen du wahrscheinlich Datenspuren hinterlässt. Wie könntest du dich schützen? Schreibe den Tagesablauf noch einmal in einer Version, in der du dich besser vor Profiling schützt.

Dabei sollst du möglichst viele der folgenden Wörter einbauen:

*App-Berechtigungen deaktivieren, Privatsphäre-Einstellungen, weniger online, Werbe-ID deaktivieren, Standortdaten ausschalten, Werbe-Blocker, Cookies löschen, Anonymes Surfen, datenschutzfreundliche Suchmaschine wie Startpage, kein offenes WLAN nutzen, Bluetooth und WLAN nur bei Benutzung aktivieren, bei Bildern die Metadaten nicht übertragen, Recht am eigenen Bild der abgebildeten Personen beachten.*

Du kannst auch nach den Begriffen im Internet recherchieren.

### Meine Datenspuren

## 5 | Datenschutzrechtliche Grundlagen – Smartphone

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS erfahren in einer praktischen Übung, wie sie ihr Smartphone datensparsam und datensicher nutzen können.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 6

### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Smartphone“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



#### Hintergrund zur Person im Video:

Miriam Meder ist Bereichsleiterin am Bayerischen Landesamt für Datenschutzaufsicht (BayLDA). Informationen unter: → [www.lida.bayern.de](http://www.lida.bayern.de)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen in der Klasse. Lösungen:

#### Aufgabe 2:

Bildschirm Sperre am Smartphone einrichten

- Starkes Passwort für Clouddienste verwenden (mindestens 10 Stellen stark)
- Werbe-ID für Android und iOS ausschalten
- Standortdaten deaktivieren
- Geotagging deaktivieren
- Alte und ungenutzte Apps löschen
- Zugriffe der Apps für jede App kontrollieren
- Betriebssystem updaten

Sammeln Sie die Tipps frontal an Tafel oder Board. Die SuS ergänzen die Aspekte auf dem Arbeitsblatt.

#### Aufgabe 3:

Die SuS führen einen der Sicherheitstipps an ihrem eigenen Smartphone durch. Über eine Recherche im Internet können sie sich Hilfe holen.

Alternativ können Sie frontal bspw. zeigen, wie man die Werbe-ID im eigenen Smartphone zurücksetzen kann. Die Werbe-ID (Android) beziehungsweise Ad-ID (iOS) hilft Anbietern aus Ihrem Nutzungsverhalten ein personalisiertes Kundenprofil zu erstellen. Eine Anleitung finden Sie z.B. unter → <https://www.connect.de/ratgeber/ad-id-zuruecksetzen-apple-ios-android-3200799.html>, (Kurzlink: <https://ogy.de/l5so>) oder → <https://mobilsicher.de/ratgeber/smartphone-nutzer-sollten-jetzt-ihre-werbe-id-aendern>, (Kurzlink: <https://ogy.de/49i1>)

**Weiterarbeit** App-Makeover! Die Sus löschen als Hausaufgabe Apps, die sie nicht mehr benötigen. Auswertung in der Folgestunde: Ist ihnen das Löschen schwergefallen?

## AB 5 | Smartphone

### Aufgabe 1:

Schaue dir das Video „Smartphone“ auf  
→ [www.datenschutz-leicht-erklaert.de/](http://www.datenschutz-leicht-erklaert.de/) an.

### Aufgabe 2:

Wie geht Paula vor, um ihr Smartphone sicher zu machen?  
Schreibe mindestens 3 Dinge auf, die du dir aus dem Video gemerkt hast.



---

---

---

---

---

---

---

---

### Aufgabe 3:

Suche dir einen der Tipps aus dem Video aus und führe ihn an deinem Smartphone durch.

### Aufgabe 4:

4. Hast du noch einen Smartphone-Sicherheits-Tipp für Paula?



---

---

---

---

---

---

---

---

## 6 | Technische Themen – Passworte

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS verstehen die Wichtigkeit von sicheren Passwörtern. In einer Praxisübung erstellen sie selbst eigene sichere Passwörter.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 6

### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Passworte“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



**Hintergrund zur Person im Video:**

Frank Spaeing ist Dozent der Initiative „Datenschutz geht zur Schule“. Informationen unter: → [www.bvdnet.de/datenschutz-geht-zur-schule/](http://www.bvdnet.de/datenschutz-geht-zur-schule/)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:

**Aufgabe 2:**

Schlechte Passworte: hallo 123, passwort, qwertz, 123456, Haseforever  
 Gute Passworte: IJ2010hibdIDgzSaDa, IGIJ2010hibdIDgzSaDa, IJ2010hibdIDgzSaDatik

**Aufgabe 3:**

- Einprägsamen Merksatz wählen und die Anfangsbuchstaben davon nehmen
- Verschiedene Passworte für verschiedenen Dienste wählen
- Passworttresor nutzen
- 12–15 Zeichen wählen
- 2-Faktor-Authentifizierung nutzen

**Hinweis:** Ein gutes Beispiel für eine 2-Faktor-Authentifizierung ist die Kombination von Bankkarte und PIN beim Geldautomaten oder von Login und Transaktionsnummer (TAN) beim Online-Banking.

**Aufgabe 4:**

Weisen Sie die SuS darauf hin, dass sie die im Unterricht erstellten und getesteten Passworte nicht für ihre privaten Accounts nutzen sollen.

**Weiterarbeit** Welche Formen von Identitätsdiebstahl es gibt, können Sie hier nachlesen und den SuS in einfachen Worten erklären: → [www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750](http://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750), (Kurzlink: <https://ogy.de/52ub>)

## AB 6 | Passworte

### Aufgabe 1:

Schaue dir das Video „Passworte“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Welches sind gute, welches schlechte Passworte?  
Streiche die schlechten durch!

IJ2010hibdIDgzSaDa

qwertz

123456

IGIJ2010hibdIDgzSaDa

Haseforever

passwort

hallo123

IJ2010hibdIDgzSaDatik



### Aufgabe 3:

Welche Tipps werden in dem Video für die Erstellung eines sicheren Passworts gegeben? Notiere.

---

---

---

---

---

### Aufgabe 4:

Erstelle selbst ein sicheres Passwort, indem du die Tipps aus dem Video berücksichtigst.  
Zeige deinem\*deiner Sitznachbar\*in das Passwort. Findet die Person heraus, welches Passwortssystem du angewandt hast? Falls ja, kannst du es vielleicht noch etwas schwieriger machen!

Mein Passwort:

---

→ <https://checkdeinpasswort.de/>

Hier kannst du dein Passwort auf Sicherheit testen. Bitte verwende das Passwort dann aber nicht mehr.  
Du kannst aber damit die Wirksamkeit der Systematik (also die Kombination aus der Länge und der Verwendung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) testen.

## 7 | Datenschutzrechtliche Grundlagen – Meine Rechte

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS erfahren, welche Datenschutzrechte sie als Verbraucher*innen haben. Sie führen ein Auskunftersuchen über die Datenspeicherung in einem selbst gewählten Online-Angebot durch. Sie berichten über ihre Erfahrungen und tauschen sich aus.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 8

### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Meine Rechte“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) auf den eigenen mobilen Geräten oder an einem PC/Tablet an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



**Hintergrund zur Person im Video:** Dr. Stefan Brink ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg. Informationen unter: → [www.baden-wuerttemberg.datenschutz.de](http://www.baden-wuerttemberg.datenschutz.de)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:

#### Aufgabe 2:

„Immer dann, wenn jemand meine Daten nutzt, muss er mich vorher darüber **informieren**, dass er das tut und auf welcher **Rechtsgrundlage**. Er darf die Daten nicht einfach nutzen, sondern er braucht dafür eine Rechtfertigung. Und diese Rechtfertigung ist oft die **Einwilligung**.“  
Frage Sie die SuS, an welcher Stelle sie bei einem Dienst diese Einwilligung gegeben haben.



#### Information: Wo befindet sich die Datenschutzerklärung?

Die Datenschutzerklärung findet sich in der Regel bei Impressum und Allgemeinen Geschäftsbedingungen (AGB) eines Dienstes im Internet. Den AGB muss man als Verbraucher/in aktiv durch ein Häkchen zustimmen, während bei der Datenschutzerklärung ein entsprechender Hinweis mit Link zur vollständigen Erklärung genügt, um der Informationspflicht gem. Art. 13, 14 DSGVO gerecht zu werden. Bei einer Datenschutzhinweis muss nur informiert werden, das heißt, es muss die Möglichkeit bestehen, dass ich sie lesen und verstehen kann. Es bedarf hier keiner Zustimmung oder aktiven Einwilligung. Viele Webseitenbetreiber stellen außerdem Datenschutzerklärungen bereit, die in die Nutzungsbedingungen oder AGB eingefügt wurden.

#### Aufgabe 3:

Richtig: Auskunftsrecht, Berichtigungsrecht, Recht auf Löschung  
Falsch: Recht auf Datenverkauf, Recht auf Verknüpfung der Datensätze in sozialen Netzwerken  
Die SuS erklären mündlich in kurzen Sätzen, was sich vermutlich hinter den einzelnen Rechten verbirgt. Erklären Sie die Rechte anschließend in einfacher Sprache, die Rechtstexte finden Sie unter folgendem Link unter Kapitel 3 in der DS-GVO, z.B. unter → <https://www.datenschutz-wiki.de>

#### **Aufgabe 4:**

Die SuS wählen einen von ihnen häufig genutzten Dienst aus und führen ein Auskunftsersuchen über die Speicherung ihrer Daten durch. Vorschläge und Anleitungen finden Sie auf dem Arbeitsblatt.

Bitte führen Sie vor der Einheit selbst einmal eine Datenauskunft durch, damit Sie Fragen der SuS beantworten können. Vorlagen für ein schriftliches Auskunftsersuchen finden Sie hier:

Muster-Auskunftsanspruch-nach-Art.-15-DS-GVO\_0621.pdf (datenschutz.de)

→ <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/06/>

**Muster-Auskunftsanspruch-nach-Art.-15-DS-GVO\_0621.pdf**, (Kurzlink: <https://ogy.de/kmgm>)

Sie können alternativ frontal zeigen, wie man eine solche Auskunft einholt. Dazu muss sich allerdings bei den meisten Angeboten eine Person bereit erklären und ihren Account zur Verfügung stellen.

Die Erfahrungen der SuS und die Auswertung der eigenen angeforderten Datensätze sollten in einer Folgestunde besprochen werden. Beachten Sie, dass im Normalfall eine Frist von einem Monat zur Beantwortung vorgesehen ist, die aber im Einzelfall verlängert werden kann.

---

#### **Weiterarbeit**

Die SuS vertiefen ihr Wissen über die Datenschutz-Grundverordnung auf dem Portal

→ <https://deinedatendeinerechte.de>. Sie können das Spiel Data Clash spielen.

---

## AB 7 | Meine Rechte

### Aufgabe 1:

Schaue dir das Video „Meine Rechte“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Ergänze die fehlenden Wörter aus dem Video  
in dem Satz:



„Immer dann, wenn jemand meine Daten nutzt,  
muss er mich vorher darüber .....,  
dass er das tut und auf welcher .....,  
Er darf die Daten nicht einfach nutzen, sondern er braucht dafür eine Rechtfertigung.  
Und diese Rechtfertigung ist in der Regel die .....“

### Aufgabe 3:

Die seit Mai 2018 zur Anwendung kommende Datenschutz-Grundverordnung (DS-GVO)  
hat einige wichtige Änderungen für uns als Verbraucher\*innen in Sachen Datenschutz gebracht.  
Welche Rechte gibt es? Welche nicht? Streiche die Rechte durch, die es nicht gibt!

- Auskunftsrecht
- Berichtigungsrecht
- Recht auf Datenverkauf
- Recht auf Löschung
- Recht auf Verknüpfung der Datensätze in sozialen Netzwerken

### Aufgabe 4:

Wir wollen uns das Recht auf Auskunft einmal genauer anschauen. Mach den **Art. 15 DS-GVO Praxistest**  
und erfahre, welche Daten der Dienst oder die Firma speichert, die du häufig nutzt. Beispiele, Vorschläge  
und Hilfen findest du hier:

- Zalando:** → [www.zalando.de/zalando-datenschutz/#chapter-11](http://www.zalando.de/zalando-datenschutz/#chapter-11) (Anleitung)
- Google:** → <https://ogy.de/10rq> (Direktlink Datenexport, Anmeldung erforderlich)
- Instagram:** → <https://ogy.de/z0ok> (Anleitung)
- Amazon:** → <https://amzn.to/3s3u4xT> (Anleitung)

Tauscht euch im Anschluss über eure Erfahrungen aus und sprecht auch darüber, ob euch bei der  
Auswertung eurer Datensätze etwas überrascht hat.

## 8 | Datenschutzrechtliche Grundlagen – Internet

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS verstehen die grundlegende Funktionsweise des Internet. Sie können die Vor- und Nachteile von IP-Abfragen erörtern.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 8

### Verlaufsplanung

<b>Einstieg</b>	Die SuS schauen sich in Einzelarbeit das Erklärvideo „Internet“ auf → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.
	<b>i</b> <b>Hintergrund zur Person im Video:</b> Frank Spaeing ist Dozent der Initiative „Datenschutz geht zur Schule“. Informationen unter: → <a href="http://www.bvdnet.de/datenschutz-geht-zur-schule/">www.bvdnet.de/datenschutz-geht-zur-schule/</a>

<b>Erarbeitung</b>	Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an, und bearbeiten die Fragen in Stillarbeit.
--------------------	---

<b>Sicherung</b>	Vergleichen Sie die Lösungen im Plenum. Lösungen: <b>Aufgabe 2:</b> Satz a) ist richtig. <b>Aufgabe 3:</b> Die SuS diskutieren darüber, in welchen Fällen es gut bzw. schlecht ist, dass über IP-Abfragen beim Provider Personen ausfindig gemacht werden können. Schlecht: Zensur der Meinungsfreiheit in Diktaturen oder totalitären Systemen. Gut: Strafverfolgung durch Polizei und Staatsanwaltschaft in Fällen von Hate Speech oder anderen Straftaten (unter Beachtung der gesetzlichen Vorgaben bei Zugriffen auf Kommunikationsdaten durch den Staat).
------------------	---

**i** **Information: Darf von den Behörden eine IP-Adresse und die/der Anschlussinhaber\*in, der/dem diese zugewiesen wurde, beim Betreiber angefordert werden?**

Liegt einer staatlichen Behörde, zum Beispiel der Polizei, eine IP-Adresse mit begründetem Verdacht auf eine Straftat vor, kann sie diese zurückverfolgen lassen. Dazu wird der jeweilige Provider (Internetanbieter z.B. Deutsche Telekom, 1&1, Vodafone, etc.) angefragt, der die Daten inklusive postalischer Adresse der/des Anschluss-Inhaber\*in nach einem richterlichen Beschluss herausgeben muss. Für normale Internetnutzer\*innen lässt sich mit einer IP-Adresse lediglich der Standort des Servers ermitteln und bis auf einige Kilometer oder eine Ortschaft eingrenzen. Mit einer bloßen E-Mail kann i.d.R die IP-Adresse der/des Kommunikationspartner\*in ermittelt werden, wenn diese in die Headerangaben eingetragen sind.

- Aufgabe 4:**
- Vermeidung von offenem WLAN
  - regelmäßiges Löschen von Cookies und anderen Internetspuren
- Die SuS können weitere Tipps hinzufügen. Recherche z.B. unter:  
→ [www.klicksafe.de/themen/datenschutz/privatsphaere/](http://www.klicksafe.de/themen/datenschutz/privatsphaere/)

<b>Weiterarbeit</b>	Wenn die SuS wissen wollen, wie ihre aktuelle IP-Adresse lautet, können sie auf dieser Webseite nachschauen: → <a href="http://www.wieistmeineip.de">www.wieistmeineip.de</a>
---------------------	---

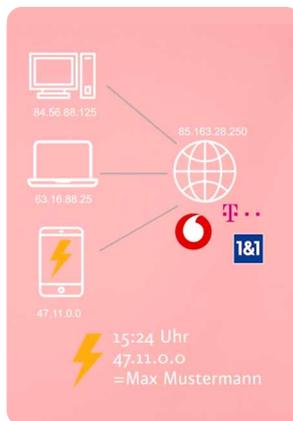
## AB 8 | Internet

### Aufgabe 1:

Schaue dir das Video „Internet“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Schaue dir die Grafik an. Welcher Satz aus dem Video unter a) bis c) ist richtig?



- a) Im Internet weiß niemand wer wir sind, nach der IP-Adresse. Das ist nur irgendeine Zahl wie 4711. Aber der Provider weiß, dass 4711 zu einem bestimmten Zeitpunkt einer bestimmten Person zugeordnet war.
- b) Wenn man einen Internetvertrag abschließt, kann man sich eine Zahl aussuchen, wie beispielsweise 4711. Die Zahl wird dann zur jeweiligen IP-Adresse. Das ist besonders praktisch, denn dann kann man die Zahl immer auswendig, wenn man die IP-Adresse auf Formularen eintragen muss.
- c) Der Administrator deines Routers kann mit dem Passwort 4711 das Internetprotokoll des letzten halben Jahres aufrufen.

### Aufgabe 3:

In welchen Fällen sollte man erfahren dürfen, wer hinter einer IP-Adresse steckt? Wann ist das angemessen und wann nicht? Tauscht euch in Kleingruppen darüber aus. Wenn ihr nicht weiter wisst, könnt ihr im Internet nach folgenden Begriffen recherchieren: *Internet-Zensur, Internetverbrechen, Hate Speech, IP-Abfrage Staatsanwaltschaft*

### Aufgabe 4:

Wie kann man weniger Spuren im Netz hinterlassen? Welche beiden Tipps werden im Video gegeben? Notiere sie und füge eigene Tipps hinzu.

---



---



---



---



---

## 9 | Technische Themen – Schutzmaßnahmen

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS lernen Maßnahmen für den Schutz ihrer Daten kennen. Sie gestalten die Tipps auf einem Informationsposter.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer; Poster
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 8

### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Schutzmaßnahmen“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



#### Hintergrund zur Person im Video:

Katarina Leikert ist Dozentin der Initiative „Datenschutz geht zur Schule“. Informationen unter: → [www.bvdnet.de/datenschutz-geht-zur-schule/](http://www.bvdnet.de/datenschutz-geht-zur-schule/)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:

#### Aufgabe 2:

1. Firewall und Antivirusprogramme aktivieren
2. Öffentliche Hotspots meiden
3. Für jede Anwendung ein anderes Passwort verwenden
4. Phishing und Anhänge in Mails nicht öffnen
5. Backups regelmäßig durchführen

Hinweis: der Tipp, einen VPN-Tunnel zu nutzen, ist sinnvoll, jedoch für SuS ohne erweiterte IT-Kenntnisse evtl. schwer zu realisieren. Vielleicht haben Sie eine\*n technikaffine\*n Schüler\*in, die\*der frontal demonstrieren kann, wie eine VPN-Verbindung eingerichtet werden kann.

#### Aufgabe 3:

Die SuS gestalten ein Poster mit den Tipps 1–5 unter Verwendung von Icons oder Symbolen. Die Poster können im Klassenzimmer aufgehängt und in einem Galeriegang betrachtet werden.

**Weiterarbeit** Die SuS können in der Analogie zum Haus im Video, das geschützt werden muss, noch weitere Beispiele aus dem Bereich Datenschutz finden. Bspw. Kidnapping mit Lösegeldforderung analog zum Erpressen von Daten durch Ransomware (Kofferwort aus „Ransom“ für Lösegeld und „Software“ für Programm).

## AB 9 | Schutzmaßnahmen

### Aufgabe 1:

Schaue dir das Video „Schutzmaßnahmen“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Welche 5 Tipps werden im Video gegeben?



Katarina Leikert, Screenshot Erklärvideo

---

---

---

---

---

### Aufgabe 3:

Erstelle ein Infoposter mit den 5 Tipps. Gestalte dein Poster, indem du passende Icons und Symbole zu jedem Tipp findest.



**i** Wenn du wissen willst, ob einer deiner Accounts von einem Hack betroffen ist, kannst du es hier checken: → <https://haveibeenpwned.com/>

Du musst dazu aber E-Mail-Adresse oder eine Telefonnummer eingeben. WICHTIG bei solchen Tools ist, dass du dabei nie dein richtiges Passwort angibst! Wenn du hörst oder liest, dass ein Unternehmen, bei dem du einen Account hast, Opfer eines Passwortabzuges wurde, solltest du dein Passwort ändern!

## 10 | Technische Themen – IT Sicherheit

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS lernen Grundlagen der IT-Sicherheit kennen. Sie intensivieren ihr Wissen, indem sie eine Anleitung zu einem der Tipps aus dem Video erstellen.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 10

### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „IT-Sicherheit“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.



#### Hintergrund zur Person im Video:

Dr. Walter Kicherer ist zuständig für den Bereich Datenschutz im Bildungswesen beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Baden-Württemberg. Informationen unter: → [www.baden-wuerttemberg.datenschutz.de](http://www.baden-wuerttemberg.datenschutz.de)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:

#### Aufgabe 2:

- Regelmäßige Betriebssystemupdates
- Regelmäßige App- bzw. Programmupdates
- Regelmäßige Datensicherung
- Vorsicht bei Link- und Dateianhängen
- WLAN-Zugang nur über WPA2 oder WPA3

**Hinweis:** der Tipp, WPA2 oder WPA3 einzurichten, ist sinnvoll, jedoch für SuS ohne erweiterte IT-Kenntnisse evtl. schwer zu realisieren. Vielleicht haben Sie eine\*n technikaffine\*n Schüler\*in, die\*der frontal demonstrieren kann, wie eine verschlüsselte WLAN-Verbindung eingerichtet werden kann.

#### Aufgabe 3:

Die SuS schreiben eine Anleitung für ihre Großeltern zu einem der Tipps. Alternativ können sie ein digitales Infoposter zu den Tipps aus dem Video erstellen und das Poster ansprechend gestalten, z.B. mit einer Poster-App wie PicCollage.

**Weiterarbeit** Die SuS recherchieren im Internet nach Folgen von digitalen Sicherheitsvorfällen ( z.B. Hackerangriff auf den Deutschen Bundestag im Jahr 2015), stellen deren Verlauf dar und erklären, durch welche Maßnahmen dies hätte verhindert werden können.

## AB 10 | IT Sicherheit

### Aufgabe 1:

Schaue dir das Video „IT-Sicherheit“ auf  
→ [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Was kannst du für deine IT Sicherheit tun?  
Notiere die Tipps aus dem Video:



Dr. Walter Kicherer, Screenshot Erklärvideo

---

---

---

---

---

### Aufgabe 3:

Schreibe zu einem der Tipps aus dem Video eine Anleitung für deine Oma oder deinen Opa.  
Formuliere es so, dass sie\*er den Tipp auch umsetzen kann.

**Alternative:** Erstelle ein digitales Poster, auf dem du die Tipps aus dem Video gestaltest.

**Anleitung:**

## 11 | Naheliegende Themen – Berufsheimnisträger

<b>Zeit</b>	45 Min.
<b>Kompetenzen</b>	Die SuS lernen Anforderungen kennen, die sich aus einer berufsrechtlichen Verschwiegenheitspflicht ergeben können.
<b>Material</b>	Webseite → <a href="http://www.datenschutz-leicht-erklart.de">www.datenschutz-leicht-erklart.de</a> ; BYOD oder PC/Tablet; Kopfhörer
<b>Zugang Internet/PC</b>	Ja
<b>Zielgruppe</b>	Ab Klasse 10

### Verlaufsplanung

**Einstieg** Die SuS schauen sich in Einzelarbeit das Erklärvideo „Berufsheimnisträger“ auf → [www.datenschutz-leicht-erklart.de](http://www.datenschutz-leicht-erklart.de) an. Dabei sollen – wenn möglich – Kopfhörer verwendet werden. Alternativ können Sie das Video auch frontal zeigen.

**i** **Hintergrund zur Person im Video:**  
 Rudi Kramer ist Sprecher der Initiative „Datenschutz geht zur Schule“. Informationen unter: → [www.bvdnet.de/datenschutz-geht-zur-schule/](http://www.bvdnet.de/datenschutz-geht-zur-schule/)

**Erarbeitung** Teilen Sie das Arbeitsblatt mit den Vertiefungsfragen zum Video aus. Die SuS schauen sich das Video evtl. ein zweites Mal an und bearbeiten die Fragen in Stillarbeit.

**Sicherung** Vergleichen Sie die Lösungen im Plenum. Lösungen:  
**Aufgabe 2:** Verschwiegenheitspflicht

**i** **§203 StGB Verletzung von Privatheimnissen**  
 Die Schweigepflicht wird auch als Verschwiegenheitspflicht oder, nach dem StGB, als Verbot der Offenbarung von Privatheimnissen genannt. Sie definiert sich als rechtliche Verpflichtung für gewisse Berufsgruppen keine Informationen an Dritte weiterzureichen, die sie im Rahmen ihrer beruflichen Tätigkeit erfahren haben. Die Heimnisträger können natürliche Personen als Berufsheimnisträger oder auch Amtsträger sein. Im letzten Fall geht es um das Amtsheimnis. Der zu Schützende wird als Heimnisherr bezeichnet, derjenige, der zur Verschwiegenheit verpflichtet ist, nennt sich Heimnisträger.  
 Quelle: <https://www.juraforum.de/lexikon/schweigepflicht>, Abruf: 3.02.2022

**Aufgabe 3:** Tierarzt und Pfarrer unterliegen dieser Schweigepflicht. Die SuS können auch selbst im Internet den Text des § 203 Abs. 1 und Abs. 2 StGB nachlesen. Klären Sie Verständnisfragen im Anschluss.

**Aufgabe 4:** Sammeln Sie mündlich weitere Personengruppen, die dem §203 StGB unterliegen. Beispiele: Berufsmäßige Gehilfen (z.B. Beschäftigte oder Auszubildende in Kanzleien oder in Praxen) und mitwirkende Personen (wie. z.B. Dienstleister). Voraussetzung: Sie müssen auf diese Verschwiegenheit verpflichtet werden.

**Aufgabe 5:** Papierentsorgung, E-Mail-Kommunikation etc. Die SuS recherchieren im Internet nach weiteren Aspekten bei denen die Verschwiegenheit zu beachten ist und erstellen eine eigene Checkliste, die sie z.B. mit ihrem Arbeitgeber besprechen können. Dies könnte folgende Bereiche betreffen: Arbeiten im Homeoffice oder auf Dienstreisen, die Nutzung von Blickschutzfolien, Telefonieren in der Öffentlichkeit, das Gespräch vor einem Sprachassistenten, der evtl. „mithört“, etc.



Quelle: Abbildung Screenshot aus dem Video

## AB 11 | Berufsgeheimnisträger

### Aufgabe 1:

Schau dir das Video „Berufsgeheimnisträger“ auf → [www.datenschutz-leicht-erklart.de/](http://www.datenschutz-leicht-erklart.de/) an.

### Aufgabe 2:

Wie nennt sich eine gesetzliche Vorgabe in Bezug auf die Vertraulichkeit bei bestimmten Berufen? Unterstreiche, was richtig ist!

- Verschwiegenheitspflicht
- Verschwiegenheitsgesetz
- Gesetz zum Schutz der Verschwiegenheit



**Aufgabe 3:** Welche der Personen sind diesem Gesetz verpflichtet? Kreuze an. Begründe, warum diese Personen dem Gesetz verpflichtet sind.

<p><a href="https://pixabay.com">https://pixabay.com</a> MaxFro</p>	<p>CC0 Public Domain</p>	<p>CC0 Public Domain</p>	<p>CC0 Public Domain</p>
BEGRÜNDUNG:			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Aufgabe 4:** Welche anderen Berufsgruppen müssen sich an die berufsrechtliche Verschwiegenheitspflicht halten? Und was ist hierfür die Voraussetzung?

**Aufgabe 5:** Bist du selbst Auszubildende\*r in einem dieser Berufe? Erstelle eine Checkliste mit den genannten Dingen aus dem Video, auf die du in deinem Betrieb achten musst, um dem §203 StGB nachzukommen.

### Checkliste

	✓



privacy4people – Gesellschaft zur Förderung des Datenschutzes gGmbH  
gGmbH des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. für gemeinnützige Projekte



DATEV-Stiftung Zukunft – Gemeinnützige Stiftung zur Förderung und Fortentwicklung von Maßnahmen in den Bereichen IT und Datenschutz, Finanz-, Steuer- und Rechtswesen sowie Genossenschaftswesen



klicksafe ist das deutsche Awareness Centre im Digital Europe Programme (DIGITAL) der Europäischen Union.

klicksafe wird gemeinsam von der Medienanstalt Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien NRW umgesetzt.



Wer noch mehr Material sucht, wird hier fündig:

 <https://www.klicksafe.de/printmaterialien/datenschutz-geht-zur-schule>



## Kontakt

Initiative „Datenschutz geht zur Schule“, BvD e. V.  
Rudi Kramer, Sprecher  
Frank Spaeing und Riko Pieper, stellv. Sprecher

Budapester Straße 31  
10787 Berlin  
Tel.: (030) 26 36 77 62  
E-Mail: kontakt@dsgzs.de  
Web: www.dsgzs.de