

Smart & Safe

Lernziele

Die SchülerInnen

- beschäftigen sich mit der Frage, welche **persönlichen Daten** warum als **sensible Daten** einzustufen sind und hinterfragen ihren **individuellen Umgang mit Daten**, die ihre eigene Person betreffen.
- werden sich dessen bewusst, dass im Zuge **mobiler Kommunikation** verschiedenste **Daten** anfallen, erfahren, in welche inhaltlichen Kategorien diese unterteilt werden, und setzen sich mit der Tatsache auseinander, dass diese Daten Rückschlüsse auf ihr soziales Umfeld bzw. ihren Tagesrhythmus ermöglichen.
- lernen die **gesetzlichen Grundlagen des Datenschutzes** kennen, übertragen diese anhand konkreter Beispiele in den Alltag und setzen sich schwerpunktmäßig mit der **Vorratsdatenspeicherung** auseinander.
- erhalten wichtige **technische Hintergrundinformationen** zum Thema „Datenschutz & Mobilkommunikation“, im Speziellen zu Möglichkeiten und Funktionsweise der **Handyortung**.
- erhalten **konkrete Tipps** für mehr Datensicherheit beim Umgang mit dem Handy.

Folgende **Kompetenzen** können erworben bzw. erweitert werden:

- Fähigkeit zur Analyse, Bewertung und Aufbereitung von **Recherche- und Umfrageergebnissen**
- Bewusster Einsatz verschiedener **Sprechhaltungen** (Information, Beschreibung, Argumentation, Appell)
- **Referieren und Argumentieren** von Sachverhalten sowie individuellen Anliegen
- **Zielgruppengerechte Aufbereitung** von Inhalten in Wort und Bild
- Formale und inhaltliche **Erschließung von Gesetzestexten**
- **Kritische Rezeption** medialer Berichterstattung
- **Vergleichen, Verbinden und Prüfen von Informationen** aus verschiedenen Textformen
- **Internetrecherche**
- **Rechnen mit Längenmaßen & Maßstäben**
- Sicherer **Umgang mit dem Handy**
- **Politische Urteilskompetenz** am Beispiel der Vorratsdatenspeicherung
- **Kommunikationsfähigkeit** über eigene Erfahrungen, technische und politische Fragestellungen und gesamtgesellschaftliche Phänomene **in englischer Sprache**

Die gewählten Methoden unterstützen den Erwerb von kommunikativer und sozialer Kompetenz sowie von Selbst- und Methodenkompetenz.

Materialien

Das Materialienpaket wurde für den Einsatz von der **6. bis 8. Schulstufe** im **interdisziplinären, bilingualen Unterricht** mit Schwerpunkt in den Fächern Deutsch, Englisch, Geographie & Wirtschaftskunde sowie Bildnerische Erziehung erstellt.

Die **Materialien in englischer Sprache** sind in der Lehrerinformation **in grüner Schrift** angeführt.



Um PädagogInnen die Abstimmung ihres Unterrichts sowohl auf den Wissensstand der SchülerInnen als auch auf aktuelle Ereignisse bzw. Medienberichte zu ermöglichen,

- liefert das Materialienpaket Anregungen für **verschiedene Einstiegs- und Abschlussvarianten** der Unterrichtseinheit, **thematische Vertiefungen** sowie unterstützende Materialien.
- wurden die Arbeitsmaterialien **methodisch vielfältig** aufbereitet. Sie können sowohl im Frontalunterricht als auch im Rahmen von Gruppenarbeiten oder bei offenem Lernen eingesetzt werden.

Weitere Informationen zum Thema finden Sie auch auf der Webseite [_bzw. auf Kinder- und Jugendschutzseiten](#) verschiedener Mobilfunkbetreiber.

Alle im Materialienpaket angeführten Weblinks wurden zuletzt am 24.5.2013 überprüft.

Einstieg

Aufbau der Unterrichtseinheit	Materialien
<p>Je nach Gruppe kann aus folgenden Einstiegsvarianten gewählt bzw. können diese kombiniert werden:</p> <p>Variante 1 – Brainstorming zum Thema</p> <p>In Gruppen oder im Klassenverband wird ein Brainstorming zum Themenkomplex „Datenschutz & Handy“ durchgeführt. Die Overheadfolie sowie die Brainstormingkarten können je nach Wissensstand der SchülerInnen als Einstiegshilfe ins Brainstorming oder – nach Durchführung und Analyse des Brainstormings – zur Vertiefung genutzt werden. Folgende Methoden bieten sich zu diesem Zweck an:</p> <p><i>Möglichkeit 1 – Brainstorming im Klassenverband anhand der Overheadfolie</i> Die SchülerInnen führen ein kurzes Brainstorming zu den auf der Folie genannten Begriff durch:</p> <ul style="list-style-type: none"> ● Welche Begriffe sind ihnen bekannt? Wenn ja – woher? ● Wie würden sie diese Begriffe definieren? ● Gibt es persönliche Erlebnisse, die sie mit diesen Begriffen verbinden? <p><i>Möglichkeit 2 – Brainstorming in Gruppen anhand der Brainstormingkarten</i> Die SchülerInnen führen in Gruppen ein kurzes Brainstorming anhand einer der Brainstormingkarten durch:</p> <ul style="list-style-type: none"> ● Ist ihnen der Begriff bekannt? Wenn ja – woher? ● Wie würden sie diesen Begriff definieren? ● Gibt es persönliche Erlebnisse, die sie mit diesem Begriff verbinden? <p>Anschließend präsentiert jede Gruppe ihr Brainstormingergebnis vor dem Klassenverband – dieses wird diskutiert, durch den Input der anderen SchülerInnen ergänzt und schlussendlich den tatsächlichen Definitionen gegenübergestellt.</p> <p>Variante 2 – Recherche zum Thema</p> <p>Die SchülerInnen erhalten die Aufgabe, jeweils einen oder mehrere der auf Overheadfolie 1 angeführten Begriffe im Internet zu recherchieren. Die Ergebnisse werden in thematischen Gruppen/im Klassenverband gesammelt, geordnet und anschließend mit den tatsächlichen Definitionen verglichen.</p> <p>Variante 3 – Analyse fiktiver Einzelfälle</p> <p>Anhand der Analyse von sechs fiktiven Fallschilderungen soll den SchülerInnen ein unmittelbarer, praxisbezogener Einstieg in die Thematik ermöglicht werden. Nach Lektüre und Einzelanalyse der verschiedenen Fallschilderungen werden folgende Fragen im Klassenverband diskutiert:</p> <ul style="list-style-type: none"> ● Welche Gemeinsamkeiten haben alle Kurzmeldungen? ● Welche Themenkomplexe lassen sich aus den Zusammenfassungen ableiten? 	<p>PRIVAT – kein Zutritt? Overheadfolie 1, Seite 28 Brainstormingkarten, Seite 30-32</p> <p>PRIVATE - no access?  Overheadfolie 1, Seite 29 Brainstormingkarten, Seite 33-35</p> <p>Schon gehört? Arbeitsblatt 1, Seite 36-38</p> <p>Have you heard?  Arbeitsblatt 1, Seite 39-41</p>

- Sind die SchülerInnen den in den Fallschilderungen dargestellten Problematiken bereits begegnet? Wenn ja – in welcher Form (mediale Berichterstattung, persönliche Betroffenheit, ...)?
- Gibt es noch weitere Themen im Zusammenhang mit „Datenschutz & Handy“, die in den Fallbeispielen nicht erwähnt und von den SchülerInnen aber als wichtig erachtet werden?

Variante 4 – Analyse von Umfrageergebnissen & Vergleich mit eigenen Erfahrungen

Jede SchülerIn erhält den Fragebogen „Ich und mein Handy“ und füllt diesen anonym aus. Anschließend stehen zwei Möglichkeiten der Auswertung zur Wahl, die entweder in Kleingruppen oder im Klassenverband durchgeführt werden können:

Möglichkeit 1:

Die SchülerInnen entwerfen in Gruppenarbeit einen Auswertungsbogen. Anschließend werden die Entwürfe miteinander verglichen. Ziel ist die Erstellung eines gemeinsamen Auswertungsbogens, anhand dessen die Ergebnisse ermittelt werden.

Möglichkeit 2:

Die Umfrageergebnisse werden mit dem Auswertungsbogen auf Arbeitsblatt 3 ermittelt.

Sobald die Ergebnisse der Klassenbefragung vorliegen, werden diese in einer offenen Diskussion mit den Ergebnissen aktueller Umfragen verglichen:

- Welche Ergebnisse sind für die SchülerInnen überraschend?
- Wo gibt es große, wo gibt es kaum Unterschiede? Wie sind diese erklärbar?

Tipp:

Geben Sie Ihren SchülerInnen die Aufgabe, die Befragung auch im Verwandten- bzw. Bekanntenkreis durchzuführen. So können die Ergebnisse der Klasse mit den Ergebnissen von Menschen mit anderen soziodemographischen Charakteristika verglichen werden.

Variante 5 – Analyse eines Zeitungsartikels

Anhand der Analyse des Zeitungsartikels „Daten frei Haus“ vom 19. Februar 2007, erschienen in der Wiener Zeitung, setzen sich die SchülerInnen mit dem Thema „Persönliche Daten & Datensicherheit“ auseinander.

Die Analyse des Artikels „Free home delivery of data“ kann mit der Vokabelübung auf Seite 2 verknüpft werden. Overheadfolie 3 liefert die Lösung.

Ich und mein Handy

Arbeitsblatt 2, Seite 42-43
Arbeitsblatt 3, Seite 46-48
Overheadfolie 2, Seite 52-53

My mobile phone and me

Arbeitsblatt 2, Seite 44-45
Arbeitsblatt 3, Seite 49-51
Overheadfolie 2, Seite 54-55



Daten frei Haus

Arbeitsblatt 4, Seite 56-58

Free home delivery of data

Arbeitsblatt 4, Seite 59-63
Overheadfolie 3, Seite 64



Overheadfolie 1/Brainstormingkarten: PRIVAT – kein Zutritt?/Private - no access

Zusatzinformation zu den angeführten Begriffen

● persönliche Daten

Als persönliche Daten bzw. „personenbezogene“ Daten werden alle Daten bezeichnet, die sich auf eine bestimmte Person beziehen. Dazu gehören Name, Adresse, Geburtsdatum und Alter ebenso wie E-Mail-Adresse oder IP-Adresse des Computers.

- **sensible Daten**

Als sensible Daten gelten laut österreichischem Datenschutzgesetz „Daten von natürlichen Personen über ihre rassistische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualeben.“¹ Sie sind Teil der persönlichen Daten.

- **Identitätsdiebstahl**

Von Identitätsdiebstahl, -betrug oder -missbrauch spricht man, wenn persönliche Daten missbräuchlich genutzt werden.

Je mehr persönliche Daten auf dem Handy gespeichert sind, zum Beispiel die Zugangsdaten zum Online-Banking, umso einfacher ist es für Handydiebe und Hacker, mit diesen Daten Schaden anzurichten.

- **gläserner Mensch**

Die Bezeichnung „gläserner Mensch“ stammt aus der Anatomie und war ursprünglich wörtlich gemeint: Sie bezog sich auf durchsichtige anatomische Kunststoffmodelle in den 1920er Jahren.

Heute wird der Begriff als Metapher für den Verlust der Privatsphäre verwendet.

- **Privatsphäre**

Unter dem Begriff „Privatsphäre“ versteht man jenen nicht-öffentlichen Bereich, in dem ein Mensch sein Recht auf freie Persönlichkeitsentfaltung ohne äußere Einflüsse wahrnehmen kann.

Das Recht auf Privatsphäre ist ein Menschenrecht und auch in den Kinderrechten verankert. So gilt das Lesen von SMS oder E-Mails als Eingriff in die Privatsphäre des Kindes. Besteht allerdings der begründete Verdacht, dass das Kind in Gefahr ist, so sind auch solche Eingriffe zulässig.

- **Handyortung**

Handys können auf verschiedenen Wegen geortet werden:

- *Ortung per Funkzelle*

Jedes Handynetz ist in Funkzellen aufgeteilt. Diese Zellen werden von einem oder mehreren Funkmasten versorgt. Sobald das Handy eingeschaltet ist, kann es einer Funkzelle oder (bei mehreren Masten) einem bestimmten Teilsegment zugeordnet werden. Der Netzbetreiber weiß damit, in welcher Zelle sich das Handy befindet.

- *Ortung per Satellit*

Handys, die mit einem GPS-Empfänger ausgestattet sind, können auch per Satellit geortet werden. Dank des GPS (Global Positioning System) kann ein Handy auch dann lokalisiert werden, wenn kein Netz verfügbar ist.

- *Ortung per Satellit und Funkzelle*

Man kann die beiden Ortungsverfahren miteinander kombinieren. In diesem Fall spricht man von A-GPS (Assisted Global Positioning System).

- *Ortung über WLAN*

WLAN-fähige Handys kann man auch über WLAN (Wireless Local Area Network) orten. Allerdings gibt es derzeit in Österreich noch keine laufend aktualisierte Karte mit allen WLAN-Netzen.

- **SPAM-SMS**

Als SPAM-SMS werden unerwünschte Textnachrichten auf dem Handy bezeichnet. Meist handelt es sich dabei um Werbe-SMS.

- **Schadprogramme**

Dieser Begriff bezeichnet Programme, die einem Handy Schaden zufügen können, wie zum Beispiel Handyviren, Trojaner und Würmer. Die Programme können sich unterschiedlich auswirken: Viren können Daten auf der Speicherkarte des Handys oder am Handy selbst löschen, Trojaner können den Akku leeren, Würmer können sich selbst als Anhang per MMS an alle Kontakte verschicken und so Kosten produzieren.

¹ www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

Datenschutzgesetz 2000; Artikel 2, Abschnitt 1

● Vorratsdatenspeicherung

Mit diesem Begriff wird die Speicherung persönlicher Daten durch oder für öffentliche Stellen bezeichnet. Vorratsdatenspeicherung deshalb, weil die Daten vorsorglich für den Fall, dass diese benötigt werden könnten, gespeichert werden. Schwere Straftaten sollen mit deren Hilfe im besten Fall verhindert bzw. Täter effektiver verfolgt und überführt werden.

Im Bereich der Mobiltelefonie umfasst die Vorratsdatenspeicherung die Speicherung der Verbindungsdaten ihrer KundInnen durch die Netzanbieter.

Nachdem sich mit Hilfe dieser Daten Profile der TelefonbesitzerInnen erstellen lassen (zum Beispiel in Hinblick auf deren Kommunikationsverhalten, deren persönliches Umfeld, ...), ist die Vorratsdatenspeicherung umstritten.

Eine EU-Richtlinie aus dem Jahr 2006⁴ verpflichtet Österreich zur Vorratsspeicherung. Nachdem der Gesetzgeber dieser Verpflichtung nicht nachgekommen ist, wurde Österreich 2010 wegen Vertragsverletzung verurteilt. 2011 wurde schließlich die Einführung der Vorratsdatenspeicherung in Österreich beschlossen und wird seit 1. April 2012 umgesetzt.

Links & Quellen zum Thema:

- www.dsk.gv.at/site/6200/default.aspx: vollständiger Gesetzestext des Datenschutzgesetzes 2000
- www.saferinternet.at/themen/datenschutz/#c723: Definition des Begriffs „persönliche Daten“
- www.kinderrechte.gv.at/home/im-fokus/kr-auf-schutz/privatsphaere/content.html: Überblicksseite zu den Kinderrechten mit einer Definition des Begriffs „Privatsphäre“
- <http://rataufdraht.orf.at/?story=15336>: Informationen für Jugendliche zur Definition der Privatsphäre in den Kinderrechten
- <http://handywissen.at/handyortung>: Fakten und Tipps zum Thema „Handyortung“
- www.elektronik-kompodium.de/sites/kom/1201061.htm: Erklärungen zu den technischen Voraussetzungen der Handyortung
- www.internet4jurists.at/provider/speicherung1a.htm: gesetzliche Grundlagen der Vorratsdatenspeicherung, Zusammenfassung der Entwicklung in Österreich

Arbeitsblatt 3: Analyse von Umfrageergebnissen & Vergleich mit eigenen Erfahrungen

Links & Quellen zum Thema:

- www.integral.co.at/downloads/Internet/2012/02/Presstext_AIM-Consumer_Q4_2011.pdf: Ergebnisse zu „beliebteste mobile Dienste“
- www.integral.co.at/downloads/Internet/2011/10/AIM-Consumer_Presstext_-_Q3_2011.pdf: Ergebnisse zu „Internet am Handy“
- www.integral.co.at/downloads/Internet/2011/07/AIM-Consumer_Presstext_-_Q2_2011.pdf: Ergebnisse zu „Smartphonebesitzer“
- www.integral.co.at/downloads/Internet/2011/03/AIM-Consumer_Presstext_2_-_Q4_2010.pdf: Ergebnisse zu „Apps“
- www.mpfs.de/fileadmin/JIM-pdf10/JIM2010.pdf: Jimstudie, deutsche Studie zur Mediennutzung Jugendlicher
- www.tarife.de/nachrichten/handy/deutsche-sind-handy-sammler_31320.html: Ergebnisse zu „Handyentsorgung“
- <http://diepresse.com/home/panorama/oesterreich/711058/Starker-Anstieg-beim-Delikt-HandyRaub-in-Oesterreich>: Artikel zu „Handyraub“
- www.rtr.at/de/komp/TKMonitor_4_2011/TM4-2011.pdf: Bericht der Rundfunk und Telekom Regulierungs GmbH, Zahlenmaterial zum Mobilfunk, unter anderem Anzahl der SIM-Karten in Österreich

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:DE:HTML> – EU Richtlinie 2006/24/EG

Arbeitsblatt 4: Daten frei Haus/Free home delivery of data

Der Artikel stammt aus der Wiener Zeitung und wurde am 19. Februar 2007 veröffentlicht.
 (www.wienerzeitung.at/nachrichten/panorama/chronik/106034_Daten-frei-Haus.html)

Zusatzinformation zu im Text angeführten Fachbegriffen

- **RFID**

RFID steht als Abkürzung für "Radio Frequency Identification", auf Deutsch Radiofrequenz-Identifikation. Diese Technik ermöglicht die automatische, berührungslose Übertragung von Daten zwischen einem Datenträger, dem so genannten Transponder, und einem Lese- und Schreibgerät mit Antenne. Mit Hilfe eines schwachen elektromagnetischen Feldes, das das Gerät mit seiner Antenne erzeugt, können Informationen zur Identifizierung und Lokalisierung von Gegenständen, Personen und Tieren kontaktlos übertragen werden. Denn sobald sich ein Transponder in den Wirkungskreis des magnetischen Feldes des Lese-/Schreibgerätes bewegt, wird der Mikrochip im Transponder mit Energie versorgt und sendet/empfängt Daten ans/vom Lese-/Schreibgerät. Entfernt sich der Transponder aus dem Magnetfeld, so bricht die Verbindung zum Lese-/Schreibgerät ab und der Mikrochip wird wieder inaktiv. Gespeicherte Daten bleiben allerdings erhalten.

Vorläufer der RFID-Technik wurden von den amerikanischen Streitkräften bereits im Zweiten Weltkrieg zur Erkennung alliierter Flugzeuge und Panzer eingesetzt.

- **Biometrie**

Der Terminus „Biometrie“ setzt sich aus zwei Begriffen griechischen Ursprungs zusammen: „Bio“ – das Leben und „Metron“ – das Vermessen. Die Biometrie ist die Lehre von der Messung an Lebewesen und beschäftigt sich zusätzlich dazu mit den verschiedenen Mess- und Auswerteverfahren, die dafür notwendig sind.




Verschiedene biometrische Verfahren ermöglichen es, Personen anhand ihrer verhaltensmäßigen und/oder biologischen Charakteristika automatisiert zu erkennen. Biologische Charakteristika sind z.B. die Gesichtsform, die Iris, die DNA, Venenmuster oder die Fingerabdrücke. Zu den verhaltensbasierten Charakteristika zählen u.a. die Stimme oder die Unterschrift.

Erfasst werden die biometrischen Merkmale über einen Scanner, anschließend werden sie in einen binären Code übertragen und verschlüsselt in einer Datenbank abgelegt. Werden neue Merkmale erfasst, so können diese mit der Datenbank verglichen und auf Übereinstimmung überprüft werden.

Links & Quellen zum Thema:

- www.dsk.gv.at: Webseite der österreichischen Datenschutzkommission
- www.brooks-rfid.com/de/rfid-grundlagen/rfid-geschichte.html: weiterführende Informationen zur RFID-Technik
- www.tagnology.com/tagnology/index.php?id=42: weiterführende Informationen zur RFID-Technik
- www.rfid-journal.de: weiterführende Informationen zu RFID
- www.ekey.net/was-ist-biometrie: Website eines europäischen Unternehmens, das sich auf Fingerprint-Zugangslösungen spezialisiert hat; auf dieser Website findet sich eine kurze allgemeine Begriffserklärung zu „Biometrie“.
- www.bromba.com/faq/biofaqd.htm#Biometrie: Website der in München angesiedelten Bromba GmbH, die im Bereich der Biometrie tätig ist; auf dieser findet sich ein umfassendes Glossar rund um „Biometrie“.

Hauptteil A

Aufbau der Unterrichtseinheit	Materialien
<p>A PERSÖNLICHE DATEN</p> <p>1. Wiederholung und Vertiefung des Verständnisses der Begriffe „persönliche“ und „sensible“ Daten</p> <p>Die Abbildungen auf Overheadfolie 3 bzw. Overheadfolie 4 sollen verdeutlichen, dass die verschiedenen Informationen zu einem Menschen und dem, was er tut, Bildpixeln entsprechen. Je mehr Pixel bzw. Daten zu einer Person bekannt sind und miteinander verknüpft werden können, umso deutlicher, präziser und aussagekräftiger wird das Bild, das man sich von dieser Person machen kann.</p> <p>Ausgehend von den Abbildungen sollen die SchülerInnen ein Brainstorming zu folgenden Fragen durchführen:</p> <ul style="list-style-type: none"> ● Welche verschiedenen Informationen gibt es zu jedem von uns? ● Sind diese Informationen bereits erfasst? Wenn ja – wo? ● Können diese von Dritten eruiert werden? Falls ja – wie? ● Welche der Informationen wurden von den SchülerInnen bereits in welchem Zusammenhang weitergegeben? ● Gibt es Informationen, die die SchülerInnen nicht weitergeben würden? Falls ja – warum nicht? <p>Anschließend können anhand Arbeitsblatt 5 die Begriffe „persönliche“ und „sensible“ Daten wiederholt und eine entsprechende Kategorisierung durchgeführt werden. Overheadfolie 4 bzw. Overheadfolie 5 liefert die Lösung.</p> <p>2. Auseinandersetzung mit dem österreichischen Datenschutzgesetz</p> <p>Die SchülerInnen erhalten die Aufgabe, die Fragen auf Arbeitsblatt 6 auf Basis einer einfachen Analyse des österreichischen Datenschutzgesetzes (DSG) zu beantworten. Dieses kann entweder selbständig recherchiert oder den SchülerInnen in der Druckvariante auf Infoblatt 1 zur Verfügung gestellt werden.</p> <p>Als Hilfestellung bei der Analyse des Datenschutzgesetzes müssen die SchülerInnen folgenden Analyseablauf einhalten:</p> <ul style="list-style-type: none"> ● <i>Schritt 1: Schriftliches Erfassen der Gliederung des Gesetzes</i> Die SchülerInnen erstellen ein Inhaltsverzeichnis – sie notieren die Überschriften der Artikel, der jeweiligen Abschnitte sowie der Paragraphen. ● <i>Schritt 2: Vergleichen der Überschriften mit den Fragestellungen und Streichung aller Artikel und Abschnitte, die für die Beantwortung der Fragestellung irrelevant sind</i> ● <i>Schritt 3: Beantwortung der Fragen auf Basis der Analyse der verbleibenden Artikel und Abschnitte</i> <p>3. Beurteilung von Fallbeispielen zur Verwendung von Daten</p> <p>Die SchülerInnen setzen sich mit der Frage auseinander, wer welche Daten wie nutzen und verwenden darf.</p>	<p>Der moderne Mensch – eine wandelnde Datenbank Overheadfolie 3, Seite 65</p> <p>The modern human being  Overheadfolie 4, Seite 66</p> <p>Achtung sensibel! Arbeitsblatt 5, Seite 67 Overheadfolie 4, Seite 69</p> <p>Caution - sensitive!  Arbeitsblatt 5, Seite 68 Overheadfolie 5, Seite 70</p> <p>Besonders schutzwürdig? Arbeitsblatt 6, Seite 71 Infoblatt Datenschutzgesetz, Seite 73-97</p> <p>Deserving special protection?  Arbeitsblatt 6, Seite 72</p> <p>Wer darf was? Arbeitsblatt 7, Seite 98-101</p>

Erst werden die entsprechenden Bestimmungen aus dem Datenschutzgesetz gelesen, und anschließend werden die auf Arbeitsblatt 7 angeführten Fallbeispiele entsprechend beurteilt.

4. Datenschutz als Selbstschutz

Bei allen gesetzlichen Regelungen liegt es nicht zuletzt in der Hand jedes Einzelnen, wie er mit seinen persönlichen Daten umgeht.

Um dieses Bewusstsein zu vermitteln, werden fünf Gruppen gebildet. Jede Gruppe erarbeitet zu einer der Aussagen auf Arbeitsblatt 8 eine Auflistung mit Argumenten für und gegen die Weiter- bzw. Bekanntgabe persönlicher Daten im jeweiligen Zusammenhang. Diese Pro- und Kontralisten werden anschließend dem Klassenverband präsentiert und gemeinsam diskutiert.

Tipp – Blindbefragung:

Führen Sie zu den fünf Themenbereichen eine Blindbefragung durch. Zu diesem Zweck müssen alle SchülerInnen die Augen schließen. Sie stellen Ihre Fragen, z.B. „Hast du eine Kundenkarte?“, „Würdest du, damit du eine Kundenkarte erhältst, deine persönlichen Daten weitergeben?“, die SchülerInnen antworten durch Handheben. Das Heben der Hand gilt als „Ja“, das Nicht-Heben als „Nein“. Die Ergebnisse werden notiert und anschließend der Klasse mitgeteilt. Gemeinsam kann diskutiert werden,

- ob dieses Ergebnis von den SchülerInnen erwartet wurde.
- ob die SchülerInnen denken, dass das Ergebnis bei einer offenen Befragung anders ausfallen würde.

Who may do what?

Arbeitsblatt 7,
Seite 102-104



Meine Daten im Ausverkauf?

Arbeitsblatt 8, Seite 105

My data for bargain-sale?

Arbeitsblatt 8, Seite 106



Overheadfolie 3 bzw. 4: Der moderne Mensch/The modern human being Arbeitsblatt 5/Overheadfolie 4 bzw. 5: Achtung – sensibel!/Caution - sensitive!

Zusatzinformation

Daten, die sich auf Personen beziehen, werden in verschiedene Kategorien eingeteilt. Die gesetzliche Grundlage für diese Kategorisierung ist das Datenschutzgesetz 2000. Das „Bundesgesetz über den Schutz personenbezogener Daten“, kurz DSGVO, regelt bzw. äußert sich zu folgenden Themen:

- Verwendung von Daten
- Datensicherheit
- Publizität der Datenverarbeitung
- Recht der Betroffenen
- Rechtsschutz
- Kontrollorgane
- Verwendungszwecke und -arten von Daten
- Videoüberwachung
- Strafbestimmungen
- Übergangs- und Schlussbestimmungen

- *„personenbezogene Daten“*
Werden in Artikel 1, Abschnitt 2, § 4 Z 1 DSGVO definiert:
„Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist.“
Damit sind Daten gemeint, die sich auf eine bestimmte Person beziehen, oder die man in Bezug zu einer ganz bestimmten Person bringen kann. Letztlich sind sehr viele Daten personenbezogen, zum Beispiel auch Einkaufsgewohnheiten oder physiologische Merkmale.
Die Bezeichnung „persönliche Daten“ wird synonym verwendet.
- *„sensible Daten“*
Werden in Artikel 1, Abschnitt 2, § 4 Z 2 DSGVO definiert:
„Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.“
Sensible Daten sind eine Unterkategorie der personenbezogenen Daten. Für sie gelten andere bzw. strengere Schutzbestimmungen als für „normale“ persönliche Daten.

Linkliste:

- www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597: Gesetzestext „Datenschutzgesetz 2000“
- http://kaernten.arbeiterkammer.at/beratung/konsumentenschutz/datenschutz/Ihr_Recht_auf_Datenschutz.html: Seite der Arbeiterkammer Kärnten zum Thema „Datenschutz“

Arbeitsblatt 6: Besonders schützenswert?/Deserving special protection?

Beantwortung der Fragen

- *Gibt es das Recht auf Geheimhaltung meiner Daten?*
Grundsätzlich ist in Artikel 1 des Datenschutzgesetzes in § 1 Abs. 1 festgehalten, dass jeder ein Recht auf Geheimhaltung der ihn betreffenden Daten hat. Allerdings muss ein schutzwürdiges Interesse bestehen. Dieses Interesse besteht nicht, „wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.“¹
- *Welcher Paragraph (§) definiert besonders schutzwürdige Daten?*
Im ersten Abschnitt in § 4 Abs. 2 werden sensible Daten als „besonders schutzwürdig“ bezeichnet.
- *Welche Paragraphen definieren Ausnahmen zu der Geheimhaltungspflicht von Daten?*
Unter bestimmten Voraussetzungen wird das Geheimhaltungsinteresse bei sensiblen und nicht-sensiblen Daten nicht verletzt. Diese Voraussetzungen sind in Artikel 2 Abschnitt 2 §§ 8 und 9 angeführt. Zum Beispiel, wenn der Betroffene die Daten selbst öffentlich gemacht hat, wenn man der Verwendung der Daten zustimmt oder wenn die Daten im öffentlichen Bereich verwendet werden, um Amtshilfe zu leisten. Amtshilfe bedeutet, dass eine Behörde eine andere Behörde unterstützt.
- *Welche Kontrollorgane gibt es in Österreich zur Wahrung des Datenschutzes?*
Die Datenschutzkommission und der Datenschutzrat sind die offiziellen Kontrollorgane. (Vgl. Artikel 2, Abschnitt 7, § 35)

¹ www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597: DSG 2000

Arbeitsblatt 7: Wer darf was?/Who may do what?

Lösung:

- *Endlich 80!*
Margit N. darf gemeinsam mit ihrer Schwester die Daten ihrer Verwandten verwenden, weil sie diese persönlich mitgeteilt bekommen hat und sie nur im familiären Zusammenhang nutzt.
→ § 45 Abs. 1





- *Spitzenangebot zum Freundes-Sonderpreis*
Bernd P. darf die Daten der Gäste nicht für seine beruflichen Aussendungen verwenden, weil er diese von den betroffenen Personen nicht persönlich mitgeteilt bekommen hat. Selbst wenn dies der Fall wäre, dürfte er die Daten nur für geschäftliche Zwecke nutzen, wenn die Betroffenen ihm dafür ausdrücklich ihre Zustimmung erteilt hätten.
→ § 45 Abs. 1 und 2

- *Information aus erster Hand*
Nadine H. darf die Daten der „Radio-Umfrage“ für eine zweite Forschungsarbeit nutzen,
 - weil diese ursprünglich auf zulässige Weise ermittelt und gesammelt wurden
 - weil diese bei der neuerlichen Nutzung anonym sind und damit kein personenbezogenes Ziel verfolgt wird.
 → § 46 Abs. 1

- *Forschen leicht gemacht!*
Nadine H. darf die Daten nicht weitergeben. Bernhard E. darf diese daher auch nicht zur Akquisition von Umfragepartnern nutzen.
→ § 47 Abs. 1

- *Zeit zum Wählen*
Nachdem an der Wahlinformation und -aufforderung öffentliches Interesse besteht, darf der Nationalrat bzw. die Nationalratspräsidentin an alle ErstwählerInnen Broschüren aussenden.
→ § 47 Abs. 2

Hauptteil B

Aufbau der Unterrichtseinheit	Materialien
<p>B DATEN RUND UMS MOBILTELEFON</p> <p>Kennenlernen der verschiedenen Daten, die ein Mobiltelefon produziert</p> <p>Overheadfolie 5 bzw. 6 gibt einen Überblick über die vier Datengruppen, die ein Mobiltelefon produziert: Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten. Im Klassenverband wird erarbeitet, welche Informationen zu welcher Datengruppe gehören.</p> <p>Anschließend werden die Tagesprotokolle auf Arbeitsblatt 9 ausgefüllt und anhand folgender Fragen analysiert:</p> <ul style="list-style-type: none"> ● Was verrät das Mobiltelefon über den Tagesablauf eines Menschen? ● Welche Rückschlüsse kann man daraus auf soziale Kontakte und tägliche Gewohnheiten eines Menschen ziehen? <p>Auf Arbeitsblatt 10 sollen die die SchülerInnen Satzteile richtig kombinieren. Diese haben die möglichen Rückschlüsse vom Telefonierverhalten eines Menschen auf dessen soziales Umfeld bzw. tägliche Gewohnheiten zum Thema.</p> <p>Auseinandersetzung mit den gesetzlichen Vorgaben</p> <p>Die SchülerInnen setzen sich mit Abschnitt 12, §§ 96-102 des österreichischen Telekommunikationsgesetzes auseinander. Diese Paragraphen widmen sich dem Kommunikationsgeheimnis und dem Datenschutz.</p> <p><i>Tipp:</i> Geben Sie Ihren SchülerInnen die Aufgabe, einzeln oder in Gruppenarbeit weitere Richtig-/Falsch-Sätze zu den Gesetzesauszügen zu erstellen. Gemeinsam kann anschließend ein Quiz durchgeführt werden.</p> <p>Vorratsdatenspeicherung</p> <ul style="list-style-type: none"> ● <i>Schritt 1 – inhaltlicher Überblick</i> Arbeitsblatt 12 liefert einen kurzen Überblick zum Thema. ● <i>Schritt 2 – Sammeln von Pro- und Kontra-Argumenten</i> Basierend auf den vorhandenen Informationen sammeln die SchülerInnen im Klassenverband oder in Gruppenarbeit Argumente für und gegen die Vorratsdatenspeicherung. <p><i>Tipp für eine Weiterführung der Sammlung von Pro- und Kontra-Argumenten mit anschließendem Rollenspiel</i> Teilen Sie Ihre SchülerInnen in vier Gruppen. Jede Gruppe erhält den Auftrag, Argumente für und gegen die Vorratsdatenspeicherung aus einer der nachfolgenden Perspektiven zu sammeln:</p> <ul style="list-style-type: none"> ○ Argumente seitens der Gesetzgebung ○ Argumente seitens der Justiz/der Exekutive ○ Argumente seitens der Mobilfunkbetreiber 	<p>Datenproduzent Handy Overheadfolie 5, Seite 107</p> <p>Mobiles Tagesprotokoll Arbeitsblatt 9, Seite 109</p> <p>The mobile phone - producer of data  Overheadfolie 6, Seite 108</p> <p>Mobile daily record  Arbeitsblatt 9, Seite 110</p> <p>Richtig kombiniert? Arbeitsblatt 10, Seite 111</p> <p>The right connection?  Arbeitsblatt 10, Seite 112</p> <p>Wer hat Zugriff? Arbeitsblatt 11, Seite 113-114 Overheadfolie 6, Seite 117</p> <p>Free access? The legal situation  Arbeitsblatt 11, Seite 115-116 Overheadfolie 7, Seite 118</p> <p>Big Brother? Arbeitsblatt 12, Seite 119</p> <p>Big Brother?  Arbeitsblatt 12, Seite 120</p> <p>Pro & Kontra Arbeitsblatt 13, Seite 121</p> <p>Pros & Cons  Arbeitsblatt 13, Seite 122</p>

Nach Abschluss des Rollenspiels werden der Diskussionsverlauf sowie die Stimmigkeit der Argumente innerhalb der Rollenspielgruppe besprochen und analysiert – das Ergebnis dieser Analyse wird den anderen Rollenspielgruppen präsentiert.

Tipp zur Erweiterung und Hinterfragung bereits gesammelter Argumente durch Recherche

Geben Sie Ihren SchülerInnen die Aufgabe, sich in den Medien zum Thema zu informieren und basierend auf diesen zusätzlichen Informationen neue Argumente zu sammeln bzw. bereits gesammelte Argumente zu hinterfragen.

- *Schritt 3 – Auseinandersetzung mit der medialen Berichterstattung rund um die Einführung der Vorratsdatenspeicherung in Österreich*
Nachdem die SchülerInnen Argumente für und gegen die Vorratsdatenspeicherung gesammelt haben, setzen sie sich abschließend mit der medialen Berichterstattung zu diesem Thema auseinander.

Die Klasse wird in sechs Gruppen geteilt. Jede Gruppe erhält einen der Presseartikel auf Arbeitsblatt 13. Die Artikel werden ausgehend von vier Analysefragen näher beleuchtet:

1. Welche Argumente werden im Artikel genannt, die für eine Vorratsdatenspeicherung sprechen?
2. Welche Argumente werden im Artikel genannt, die gegen eine Vorratsdatenspeicherung sprechen?
3. Wie gut informiert fühlt man sich nach dem Lesen des Artikels?
4. Stimmen die im Artikel angeführten Informationen zur Vorratsdatenspeicherung beim Telefon?

Die Ergebnisse der einzelnen Gruppen werden miteinander verglichen. Abschließend können die aus den Artikeln gesammelten Argumente mit jenen der SchülerInnen verglichen werden.

Tipp:

Erfolgt die Analyse der Zeitungsartikel im Stationenbetrieb, so können die SchülerInnen die einzelnen Artikel auch direkt miteinander vergleichen.

Tipp zur Internationalisierung des Themas „Vorratsdatenspeicherung“ am Beispiel Deutschland

Ausgangspunkt für die Einführung der Vorratsdatenspeicherung in Österreich ist eine EU-Richtlinie aus dem Jahr 2006. Diese gilt für alle EU-Mitgliedsstaaten.

Geben Sie den SchülerInnen die Aufgabe zu recherchieren, wie die Richtlinie in Deutschland umgesetzt wurde, und welche Entwicklung es dort bis zum jetzigen Zeitpunkt gegeben hat.

Gut informiert?

Arbeitsblatt 14,
Seite 123-132

Overheadfolie 5 bzw. 6: Datenproduzent Handy/The mobile phone - producer of data

Zusatzinformation

Im Telekommunikationsgesetz wird unter anderem definiert, welche Daten ein Mobiltelefon erzeugt und wie diese bezeichnet werden. Nachfolgend die entsprechenden Auszüge aus dem Telekommunikationsgesetz:

„*Stammdaten*“ sind alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

- Familienname und Vorname,
- akademischer Grad,
- Wohnadresse,
- Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
- Information über Art und Inhalt des Vertragsverhältnisses,
- Bonität

„*Verkehrsdaten*“ sind Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Zu den Verkehrsdaten zählen auch die „*Zugangsdaten*“, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.

„*Standortdaten*“ sind Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben.

„*Inhaltsdaten*“ sind die Inhalte übertragener Nachrichten.

Als „*Nachricht*“ gilt jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können.

Dem Kommunikationsgeheimnis unterliegen die Verkehrsdaten, die Standortdaten und die Inhaltsdaten: Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

Quelle: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849
– vollständige Fassung des Telekommunikationsgesetzes vom 15.05.2013

Arbeitsblatt 9: Mobiles Tagesprotokoll/Mobile daily record

- Quelle Studie Marketagent:
<http://derstandard.at/1285199348055/Jugendstudie-Schlussmachen-per-SMS-bei-717-Prozent-verpoent>
- Quelle Handybesitz: www.oe24.at/digital/Nur-2-Prozent-wollen-ohne-Handy-leben/813578

Arbeitsblatt 10: Richtig kombiniert?/The right connection?

Lösung:

- Wenn jemand weiß, mit wem du telefonierst, kann er daraus auf deinen Freundes- und Bekanntenkreis schließen.
- Wer über die zeitliche Nutzung deines Handys Bescheid weiß, ist auch über deinen Tagesablauf informiert.
- Wie oft und wie lang du mit jemandem telefonierst, zeigt, wie wichtig dir diese Person ist.
- Wo du den lieben langen Tag unterwegs bist, kann man aus den Standortdaten deines Handys ablesen.
- Die Verkehrs- und Standortdaten deines Telefons verraten nichts über Gesprächs- oder Nachrichteninhalte.

Arbeitsblatt 12: Big Brother?/Big Brother?

Arbeitsblatt 14: Gut informiert?

Zusatzinformation

- **Die Debatte rund um die Vorratsdatenspeicherung in Österreich**

Der folgende Auszug aus dem österreichischen Telekommunikationsgesetz definiert nicht nur die Daten, die im Zusammenhang mit Telefondiensten im Rahmen der Vorratsdatenspeicherung gesammelt werden, sondern auch jene Daten, die Internet-Anbieter sowie Anbieter von E-Mail-Diensten sammeln müssen.

Vorratsdaten

- § 102a.** (1) Über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus haben Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt.
- (2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:
1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
 2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
 3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
 4. die eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist.
- (3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:
1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
 2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
 3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;
 4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;
 5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimedia-dienste).
 6. Bei Mobilfunknetzen zudem
 - a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;
 - b) der internationalen Mobilfunkgeräteerkennung (IMEI) des anrufenden und des angerufenen Anschlusses;
 - c) Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;
 - d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.
- (4) Anbietern von E-Mail-Diensten obliegt die Speicherung folgender Daten:
1. die einem Teilnehmer zugewiesene Teilnehmerkennung;
 2. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war;
 3. bei Versenden einer E-Mail die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail-Adresse jedes Empfängers der E-Mail;
 4. beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail-Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;
 5. bei An- und Abmeldung beim E-Mail-Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrunde liegenden Zeitzone.
- (5) Die Speicherpflicht nach Abs. 1 besteht nur für jene Daten gemäß Abs. 2 bis 4, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden. Im Zusammenhang mit erfolglosen Anrufversuchen besteht die Speicherpflicht nach Abs. 1 nur, soweit diese Daten im Zuge der Bereitstellung des betreffenden Kommunikationsdienstes erzeugt oder verarbeitet und gespeichert oder protokolliert werden.

- (6) Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 34 KommAustriaG unterliegen.
- (7) Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden.
- (8) Die nach Abs. 1 zu speichernden Daten sind nach Ablauf der Speicherfrist unbeschadet des § 99 Abs. 2 unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen. Die Erteilung einer Auskunft nach Ablauf der Speicherfrist ist unzulässig.
- (9) Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO.

Auskunft über Vorratsdaten

- § 102b.** (1) Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig.
- (2) Die nach § 102a zu speichernden Daten sind so zu speichern, dass sie unverzüglich an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.
 - (3) Die Übermittlung der Daten hat in angemessen geschützter Form nach Maßgabe des § 94 Abs. 4 zu erfolgen.

Datensicherheit, Protokollierung und Statistik

- § 102c.** (1) Die Speicherung der Vorratsdaten hat so zu erfolgen, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist. Die Daten sind durch geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen. Ebenso ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips vorbehalten ist. Die Protokolldaten sind drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSGVO 2000 zuständigen Datenschutzkommission. Eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit kann der Bundesminister für Verkehr, Innovation und Technologie per Verordnung festschreiben.
- (2) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben zu gewährleisten, dass jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten nach § 102b revisions sicher protokolliert wird. Diese Protokollierung umfasst
 - 1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
 - 2. in den Fällen des § 99 Abs. 5 Z 3 und 4 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
 - 3. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
 - 4. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze,
 - 5. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung,
 - 6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie
 - 7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.
 - (3) Die Speicherung der Protokolldaten hat so zu erfolgen, dass deren Unterscheidung von Vorratsdaten sowie von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherter Daten möglich ist.
 - (4) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben
 - 1. für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit die Protokolldaten gemäß Abs. 2 an die Datenschutzkommission und den Datenschutzrat sowie
 - 2. zum Zweck der Berichterstattung an die Europäische Kommission und an den Nationalrat die Protokolldaten gemäß Abs. 2 Z 2 bis 4 an den Bundesminister für Justiz zu übermitteln.

- (5) Die Übermittlung der Protokolldaten hat auf schriftliches Ersuchen der Datenschutzkommission bzw. des Bundesministers für Justiz zu erfolgen; die Übermittlung an den Bundesminister muss darüber hinaus jährlich bis zum 31. Jänner für das vorangegangene Kalenderjahr erfolgen.
- (6) Über die Protokollierungspflichten nach Abs. 2 hinaus ist eine Speicherung der übermittelten Datensätze selbst unzulässig.

In Österreich gibt es massive Kritik an der Vorratsdatenspeicherung. Von Gegnern wird sie als massiver, unzulässiger Eingriff in die Freiheit und Privatsphäre der ÖsterreicherInnen empfunden.

Linksammlung zu kritischen Stimmen zur Vorratsdatenspeicherung in Österreich:

- <http://akvorrat.at>: Bürgerinitiative gegen die Vorratsdatenspeicherung
- www.argedaten.at/php/cms_monitor.php?q=DATA-RETENTION: Informationsseite der „ARGE-Daten“ zur Vorratsdatenspeicherung

● Die Vorratsdatenspeicherung im EU-Zusammenhang

Die Idee, Kommunikationsdienste zur Speicherung von Daten zu verpflichten, um bei Bedarf darauf zurückgreifen zu können, wurde von der EU nach den Terroranschlägen 2005 in London massiv vorangetrieben. Dahinter steckt der Wunsch, Daten zu sichern, die zur Auflösung oder im besten Fall zur Verhinderung von Verbrechen dienen sollen. Die EU-Richtlinie 2006/24/EG äußert sich „über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden“¹ und gibt einen groben Rahmen vor, welche Daten für welchen Zeitraum gespeichert werden sollen. Die Umsetzung der Richtlinie bleibt den jeweiligen Mitgliedsstaaten überlassen.

Die im März 2006 beschlossene Verordnung war von den Mitgliedsstaaten bis September 2007 umzusetzen, bezüglich der Internetdaten galt die Frist bis März 2009.

○ *Entwicklung in Österreich*

Das BMVIT (Bundesministerium für Verkehr, Innovation und Technologie) hat im April 2007 einen entsprechenden Entwurf des Telekommunikationsgesetzes (TKG) ausgearbeitet und ein Begutachtungsverfahren eingeleitet. Allerdings konnte sich die Regierung auf keine Umsetzung einigen. Ein Vorwurf von Kritikern war z.B., dass der österreichische Entwurf zur Vorratsdatenspeicherung umfangreicher ausgefallen wäre als in der EU-Richtlinie vorgegeben. 2009 kam der nächste Entwurf, zu dem ebenfalls ein Begutachtungsverfahren eingeleitet wurde. Wieder gab es keine Einigung.

2010 wurde Österreich wegen Vertragsverletzung vom europäischen Gerichtshof verurteilt. 2011 wurde schließlich die Novelle des Telekommunikationsgesetzes verlautbart, die am 1. April 2012 in Kraft getreten ist.

○ *Entwicklung in Deutschland*

In Deutschland wurde die Vorratsdatenspeicherung bereits 2004 und 2005, also noch vor Beschluss der EU-Richtlinie diskutiert, aber beide Male abgelehnt. Die EU-Richtlinie zur Vorratsdatenspeicherung aus dem Jahr 2006 wurde 2007 in einem Gesetzestext verarbeitet. Das Gesetz wurde im selben Jahr verabschiedet und trat am 1.1.2008 in Kraft.

Gegen das neue Gesetz wurden 2007 und 2008 drei Verfassungsbeschwerden beim Bundesverfassungsgericht eingereicht.

2010 verkündete das deutsche Verfassungsgericht, dass die Vorratsdatenspeicherung nicht mit dem deutschen Grundgesetz vereinbar ist. Seither gibt es (Stand: April 2012) in Deutschland kein gültiges Gesetz zur Regelung der Vorratsdatenspeicherung. Die EU hat Deutschland aufgefordert, eine Vorratsdatenspeicherung schnellstmöglich wieder einzuführen und eine Frist bis zum 26. April 2012 gesetzt. Einen Gesetzesentwurf des deutschen Bundesjustizministeriums lehnte das Innenministerium am 16. April 2012 ab.

¹ www.internet4jurists.at/gesetze/rl_vorratsdaten01.htm – EU Verordnung 2006/24/EG

○ Reaktionen der EU

Die EU-Kommission hat mittlerweile eine Prüfung der Richtlinie zu den Vorratsdaten durchgeführt. Dazu gab Innenkommissarin Malmström im April 2011 folgendes Statement ab:

„Unsere Prüfung hat gezeigt, dass die Richtlinie in den verschiedenen EU-Ländern unterschiedlich umgesetzt worden ist“, sagte Innenkommissarin Cecilia Malmström der „Welt“. „Das ist zwar grundsätzlich für die Umsetzung von EU-Recht nicht ungewöhnlich. Aber ich glaube, dass die derzeitige Richtlinie den Regierungen zu viel Spielraum bei der Umsetzung der Vorratsdatenspeicherung gibt. Auch lässt sie zu viel Raum für die Aufbewahrung und den Umgang der Telekommunikationsanbieter mit den Daten.“ Zudem sei der Rahmen, in dem sich Strafverfolger Zugang zu diesen Daten beschaffen können, zu groß.“²

Eine neue Richtlinie wurde bislang nicht bekanntgegeben. Am 16. April 2013 hat die EU-Kommission allerdings beschlossen, eine neue Expertengruppe zur Vorratsdatenspeicherung einzusetzen. (Stand: Mai 2013)

Linksammlung zur Vorratsdatenspeicherung im EU-Zusammenhang:

- <http://register.consilium.eu.int/pdf/de/05/st03/st03677.de05.pdf>: EU-Richtlinie zur Vorratsdatenspeicherung
- www.bfdi.bund.de/cln_007/nn_533578/DE/Schwerpunkte/Vorratsdaten/Artikel/Vorratsdatenspeicherung.html: offizielle Seite des Bundesbeauftragten für Datenschutz in Deutschland
- www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html: Urteil des Bundesverfassungsgerichts vom 2. März 2010
- www.spiegel.de/netzwelt/netzpolitik/0,1518,681122,00.html: Artikel zur Entscheidung des deutschen Verfassungsgerichts 2010
- www.spiegel.de/politik/ausland/0,1518,757499,00.html: Artikel zur Aufforderung der EU an Deutschland, die Vorratsdatenspeicherung wieder einzuführen
- www.fnp.de/fnp/nachrichten/politik/innenministerium-lehnt-fdpentwurf-zu-vorratsdaten-ab_rmn01.c.9764503.de.html: Artikel zur Frist bis 26.4.2012 in Deutschland
- <http://fm4.orf.at/stories/1716492>: Artikel zur Ausweitung der Vorratsdatenspeicherung auf Soziale Netzwerke vom 22.4.2013

² www.welt.de/print/die_welt/politik/article13179292/Bruessel-will-neue-Regeln-fuer-Vorratsdaten-erlassen.html

Hauptteil C

Aufbau der Unterrichtseinheit	Materialien
<p>C HANDYORTUNG</p> <p>Technische Grundlagen der Handyortung</p> <p>Auf Arbeitsblatt 15 werden die beiden grundlegenden Varianten der Handyortung erklärt: die Ortung via Funkzelle sowie die Ortung via Satellit.</p> <p>Die Rechenaufgaben auf Seite 2 verdeutlichen, dass Funkzellen unterschiedlich groß sein können. Gleichzeitig wiederholen die SchülerInnen das Umrechnen von Maßstäben und Maßeinheiten.</p> <p><i>Tipp:</i> Im Anschluss an die Rechenaufgaben kann auf www.senderkataster.at die Anzahl der Sendemasten für den Schulstandort bzw. den Wohnort der SchülerInnen ermittelt und die durchschnittliche Größe einer Funkzelle errechnet werden.</p> <p>Anwendungsgebiete der Handyortung</p> <p>Auf Overheadfolie 7 bzw. 8 sind die unterschiedlichen Anwendungsgebiete der Handyortung grafisch dargestellt. Im Klassenverband werden folgende Fragen diskutiert:</p> <ul style="list-style-type: none"> • Wer von den SchülerInnen nützt ein Angebot, das auf Handyortung basiert? • Welche Angebote werden von den SchülerInnen genutzt? • Welche Angebote sind für welche Zielgruppe sinnvoll? • Welche Angebote sind potenziell problematisch? <p>Bewusstmachung potenzieller Problemfelder der Handyortung ausgehend vom unmittelbaren Lebenszusammenhang der SchülerInnen</p> <p>Die SchülerInnen verfassen eine Kurzgeschichte, die eine negative Auswirkung der Ortungsfunktion zum Thema hat.</p> <p>Als Einstiegshilfe in die kreative Auseinandersetzung liefert Arbeitsblatt 16 alternativ zwei mögliche Einstiege in die Kurzgeschichte.</p>	<p>Gewusst wie?</p> <p>Arbeitsblatt 15, Seite 133-135</p> <p>Know how!</p> <p>Arbeitsblatt 15, Seite 136-138 </p> <p>Handyortung - 7 Fliegen auf einen Streich</p> <p>Overheadfolie 7, Seite 139</p> <p>Know how!</p> <p>Overheadfolie 8, Seite 140 </p> <p>Es war einmal ...</p> <p>Arbeitsblatt 16, Seite 141</p> <p>Once upon a time ...</p> <p>Arbeitsblatt 16, Seite 142 </p>

Arbeitsblatt 15: Gewusst wie!/Know how!

- Lösung zur Frage: „Wirkt sich die Größe einer Funkzelle auf das Ergebnis der Handyortung aus?“
Ja – die Größe der Funkzelle wirkt sich auf das Ortungsergebnis aus. Denn bei der Handyortung über Funkzellen kann nur die Funkzelle, in der sich das Handy befindet, geortet werden. Der exakte Aufenthaltsort des Handys innerhalb dieser Funkzelle bleibt unbekannt. Je größer die jeweilige Funkzelle ist, in der sich das gesuchte Handy befindet, umso ungenauer wird daher das Ortungsergebnis.

- *Lösungen zur Errechnung verschiedener Funkzellengrößen*

- **Beispiel 1: dicht besiedelte Großstadt**

Auf dem Kartenausschnitt sind 4.000 m² abgebildet ($8 \cdot 5 \cdot 10.000/100$), das entspricht 4 km². Insgesamt sind 74 Sendemasten abgebildet. Daraus ergibt sich eine durchschnittliche Fläche von 54,05 m², die ein Sendemast in dieser Gegend abdeckt.

- **Beispiel 2: Stadt**

Auf dem Kartenausschnitt sind 26.000 m² abgebildet ($8 \cdot 5 \cdot 65.000/100$), das entspricht 26 km². Insgesamt sind 21 Sendemasten abgebildet. Daraus ergibt sich eine durchschnittliche Fläche von 1,24 km², die ein Sendemast in dieser Gegend abdeckt.

- **Beispiel 3: Land**

Auf dem Kartenausschnitt sind 96.000 m² abgebildet ($8 \cdot 5 \cdot 240.000/100$), das entspricht 96 km². Insgesamt sind 14 Sendemasten abgebildet. Daraus ergibt sich eine durchschnittliche Fläche von 6,86 km², die ein Sendemast in dieser Gegend abdeckt.

Tipp:

In diesem inhaltlichen Zusammenhang können auch **Übungen zum Umrechnen von Watt** durchgeführt werden.

Die vom Forum Mobilkommunikation herausgegebene Broschüre „Sicherheit. Transparenz. Verantwortung“ (www.senderkataster.at/Messbroschuere.pdf) enthält nicht nur die österreichweit geltenden Grenzwerte für Immissionen von Mobilfunkanlagen, sondern auch konkrete Messergebnisse vom TÜV Austria. In 106 österreichischen Gemeinden wurden im Jahr 2009 255 öffentlich zugängliche, zentral gelegene und gut frequentierte Plätze auf die dortigen Hochfrequenz-Immissionen getestet. Die Ergebnisse ausgewählter Messpunkte können gemeinsam mit den SchülerInnen verglichen und die Watt-Werte/m² in Milli- und Microwatt umgerechnet werden.

Falls Sie sich mit Ihren SchülerInnen intensiver mit der **Funktionsweise von Handys und Mobilfunknetzen** auseinandersetzen möchten, steht Ihnen das Unterrichtsmaterialienpaket „**Strahlemann**“ auf www.lehrer.at/handy zum kostenlosen Download zur Verfügung.

Zusatzinformation

- **Ortung per Funkzelle**

Jedes Mobilfunknetz besteht aus aneinander angrenzenden Funkzellen. Eine Funkzelle ist ein Bereich, in dem sich jeweils eine Sende- und Empfangsstation befindet, eine sogenannte Mobilfunkbasisstation. Die Größe einer Funkzelle ist abhängig von der Anzahl der erwarteten TeilnehmerInnen, dem Bebauungsgrad, der Landschaft und der eingesetzten Mobilfunktechnologie. UMTS-Anlagen haben eine geringere Reichweite als GSM-Anlagen.

In dicht besiedeltem Gebiet beträgt der Durchmesser einer Funkzelle zwischen 300 und 500 Meter, auf dem Land können dies auch zwei bis drei Kilometer sein. Damit bestehende Gespräche nicht abgebrochen werden, wenn man eine Funkzelle verlässt, müssen sich die Funkzellen leicht überlappen. Sobald das Handy eingeschaltet ist, kann es einer Funkzelle oder (bei mehreren Masten) einem bestimmten Teilsegment zugeordnet werden. Der Netzbetreiber weiß, in welcher Zelle sich das Handy befindet.

- **Ortung per Satellit**

Handys, die mit einem Satelliten-Navigationsempfänger ausgestattet sind, können via Satellit ihren Aufenthaltsort bestimmen. Für den Empfang und die Auswertung der Satellitendaten ist kein Netz notwendig. Die Lokalisierung basiert auf der Laufzeit des Signals eines Satelliten. Kennt man die Laufzeit des Signals kann man die Entfernung zwischen Satellit und Empfänger des Signals berechnen. Um einen Standort bestimmen zu können, braucht man Laufzeitmessungen von mindestens zwei Satelliten. So erhält man Radiuskurven, die sich an einem Punkt überschneiden. An diesem Punkt befindet sich der Empfänger des Signals – die Ortung war erfolgreich.

Die Übermittlung dieser Ortungsdaten an Dritte ist allerdings nur möglich, wenn das Handy über Mobilfunkempfang verfügt, ohne Netz können die Positionsdaten nicht an Dritte weitergegeben werden.

Spricht man von Satelliten-Navigationssystemen, denkt man üblicherweise nur an „GPS“. GPS ist die Abkürzung für „Global Positioning System“. Insgesamt umrunden derzeit (Stand: April 2012) 27 solarbetriebene GPS-Satelliten in ca. 20.200 km Höhe mit einer Geschwindigkeit von 3,9 km pro Sekunde die Erde. Ihre Umlaufzeit beträgt 11 Stunden und 58 Minuten.

24 dieser Satelliten schicken ihre Signale an die Erde, die verbleibenden drei sind Ersatzsatelliten, die aktiviert werden, wenn ein Satellit ausfällt. Die Satelliten sind so angeordnet, dass an jedem Punkt der Erde zumindest vier Satelliten zeitgleich empfangen werden können.

GPS ist allerdings nicht das einzige Satelliten-Navigationssystem. Auch Europa und Russland haben eigene Systeme entwickelt. Das europäische Satelliten-System heißt „Galileo“ und wurde als einziges zu zivilen Zwecken und nicht für den militärischen Einsatz entwickelt. „Galileo“ ist noch sehr jung, der Testbetrieb wurde erst 2011 aufgenommen. Das russische System heißt „GLONASS“.

- **Ortung per Satellit und Funkzelle**

Die beiden Ortungsverfahren via Satellit und Funkzelle können miteinander kombiniert werden. In diesem Fall spricht man von A-GPS (Assisted Global Positioning System).

- **Ortung über WLAN**

WLAN-fähige Handys kann man auch über WLAN (Wireless Local Area Network) orten. Allerdings gibt es derzeit in Österreich noch keine laufend aktualisierte Karte mit allen WLAN-Netzen.

Linksammlung:

- www.gps.gov: offizielle Website der US-amerikanischen Regierung zu GPS
- www.thomas-wilhelm.net/arbeiten/ZulaGPS.pdf: schriftliche Hausarbeit von Matthias Braun zum Thema „Das GPS-System – Funktionsweise und Einsatzmöglichkeiten im Physikunterricht“ aus dem Jahr 2007; diese Arbeit bietet zahlreiche inhaltliche Ansätze zur Vertiefung des Themas im Physikunterricht.
- www.hs-esslingen.de/~abel/gps/Abel-GPS.htm: ein Beitrag zu Funktionsweise und mathematischen Grundlagen von GPS verfasst von Heinrich Abel (Esslingen)
- http://eu.mio.com/de_de/global-positioning-system_4985.htm: Infoseite des Navigationslösungsanbieters Mio
- www.kowoma.de/gps/Positionsbestimmung.htm: weiterführende Informationen zur Positionsbestimmung über GPS
- www.elektronik-kompodium.de/sites/kom/1201071.htm: allgemeine Infos zu GPS
- http://ec.europa.eu/enterprise/policies/satnav/index_de.htm: Informationen zum europäischen Satelliten-Navigationssystem „Galileo“
- www.galileo-navigationssystem.com: Informationen zu „Galileo“
- www.glonass-ianc.rsa.ru/en: Informationen zum russischen Satelliten-Navigationssystem „GLONASS“
- www.wissen.de/lexikon/satellit-raumfahrt?keyword=Nachrichtensatellit: Informationsseite zu Satelliten

Overheadfolie 7 bzw. 8: Handyortung - 7 Fliegen auf einen Streich/Know how!

Zusatzinformationen:

Navigation: Sowohl Handyhersteller als auch Firmen, die sich auf Navigationslösungen spezialisiert haben, haben sich auf die Generation der Smartphones eingestellt und entsprechende Navigationssoftware erstellt, die entweder bereits am Handy vorinstalliert ist oder als App zum Download angeboten wird.

Lost and found: Die Standortbestimmung kann man sich auch bei verlorenen oder gestohlenen Handys zunutze machen. So gibt es zum Beispiel Schutzprogramme, die im Fall eines Verlustes oder Diebstahls den Standort des Handys melden. Sicherheitsfirmen bieten solche Ortungsdienste an. Eines davon ist das Programm „Anti-Theft for Mobile“ von F-Secure. Dieses stellt per SMS an das verlorene bzw. gestohlene Handy fest, wo sich dieses befindet, und kann das Telefon bei Bedarf sogar aus der Ferne sperren bzw. alle Daten löschen.

Notfälle: Die Standortdaten jedes eingeschalteten Handys sind dem Netzbetreiber bekannt und werden im Falle eines Notfalls auch weitergegeben. Ist keine aktuelle Ortung möglich, dürfen die Netzbetreiber auf den letzten bekannten Standort, der im Rahmen der Vorratsdatenspeicherung erfasst wurde, zugreifen.

Verbrechensverfolgung: Die Standortdaten eines Handys werden aufgrund der Vorratsdatenspeicherung für sechs Monate gespeichert und können im Rahmen polizeilicher Ermittlungen eingesehen werden.

Schutzfunktionen: Für hilfsbedürftige Menschen, Kinder oder auch Tiere werden Ortungssysteme angeboten, die im Falle eines „Verschwindens“ eine schnelle Übermittlung des Aufenthaltsortes der gesuchten Person ermöglichen.

Sightseeing & Shopping: Es gibt zahlreiche Apps, die Informationen zu den Sehenswürdigkeiten, Shops oder Sonderangeboten in der näheren Umgebung liefern. Zu diesem Zweck wird der Standort des Handys ermittelt, mit Datenbanken abgeglichen, um schlussendlich die dem Standort entsprechenden Informationen an das Handy zu übertragen.

Soziale Netzwerke: Viele Onlinecommunities bieten Funktionen an, die sich auf den eigenen Standort beziehen. So kann man als Mitglied einer Social Community zum Beispiel die Funktion aktivieren, dass die Position des Handys bei jeder Aktualisierung des Profils oder auch bei jedem Posting automatisch ermittelt und auf der eigenen Profilseite angegeben wird.

Linksammlung:

- www.f-secure.com/de/web/home_de/protection/anti-theft-for-mobile/overview: Handyortung von F-Secure, Gratisdownload
- www.kaspersky.com/de/kaspersky-mobile-security: Handyortung über Kaspersky lab
- www.facebook.com/about/location: Infoseite zu „facebook – places“

Hauptteil D

Aufbau der Unterrichtseinheit	Materialien
<p>D ANGRIFFE VON DRITTEN</p> <p>Kennenlernen potenzieller Sicherheitslücken</p> <p>Arbeitsblatt 17 vermittelt einen ersten Überblick über mögliche Sicherheitsrisiken, die mit der Nutzung eines Mobiltelefon, insbesondere eines Smartphones, verbunden sind.</p> <p>Der Text ist in zwei Versionen vorhanden:</p> <ul style="list-style-type: none"> ● <i>Version 1:</i> Die SchülerInnen ordnen den beschriebenen Sicherheitsrisiken die richtige Bezeichnung zu. ● <i>Version 2:</i> Die SchülerInnen ordnen den beschriebenen Sicherheitsrisiken die richtige Bezeichnung zu und wiederholen gleichzeitig die s-Schreibung. ● <i>Version 2:</i> Die SchülerInnen ordnen den beschriebenen Sicherheitsrisiken die richtige Bezeichnung zu und ergänzen die fehlenden Verbformen. Anschließend kann noch eine Übung zur Bildung verschiedener Verbformen angeschlossen werden. (Seite 4) <p>Overheadfolie 8 bzw. 9 liefert die Lösung zur Textvariante 2.</p> <p>Im Anschluss an die Ergänzungsübung können die Verständnisfragen auf Seite 4 des Arbeitsblattes im Klassenverband, in Gruppen oder einzeln beantwortet werden.</p> <p>Recherche von Schutzmaßnahmen & Aufbereitung eines Infoblattes</p> <p>Die SchülerInnen werden in vier Gruppen geteilt, die sich in Folge jeweils mit einem der Themenbereiche Apps, Bluetooth & Infrarotschnittstellen, WLAN und Schadsoftware näher beschäftigen.</p> <p>In einem ersten Schritt gilt es, Schutzmaßnahmen im jeweiligen Bereich zu recherchieren. Alternativ zur Recherche können diese auch dem Infoblatt 2 entnommen werden.</p> <p>Anschließend werden die Sicherheitsrisiken sowie entsprechende Schutzmaßnahmen in Form eines Infoblattes für die Zielgruppe „SeniorInnen 70+“ aufbereitet. Das heißt, die SchülerInnen müssen davon ausgehen, dass wenig Detailwissen zu modernen Mobilfunkanwendungen vorhanden ist. Grafische Elemente sind erlaubt, aber nicht vorgeschrieben.</p> <p>Das Infoblatt soll folgende Struktur bzw. Inhalte aufweisen:</p> <ol style="list-style-type: none"> 1. <i>Titel bzw. Slogan</i> 2. <i>Teaser:</i> kurze Einführung in den Themenbereich, z.B. in Form einer Fallschilderung 3. <i>Beschreibung des konkreten Sicherheitsrisikos:</i> Worin liegt das Risiko? Welcher Schaden kann der HandyuserIn entstehen? Wie kann es zu solchen Sicherheitslücken kommen? 4. <i>Schutzmaßnahmen:</i> einfache, konkrete Handlungsanleitungen für die InfoblattleserInnen 	<p>Alles sicher?</p> <p>Arbeitsblatt 17, Seite 143-146 Overheadfolie 8, Seite 147</p> <p>All safe?</p> <p>Arbeitsblatt 17, Seite 148-152 Overheadfolie 9, Seite 153</p> <p>Schutzschild aktiv?</p> <p>Infoblatt 2, Seite 154-163</p> <p>Mobile phone security</p> <p>Infoblatt 2, Seite 164-167</p>



Achtung:

Weisen Sie Ihre SchülerInnen darauf hin, dass es nicht darum geht, Angst zu schüren, sondern Sicherheit durch konkrete Handlungsanleitungen zu vermitteln.

Sind alle Infoblätter fertiggestellt, werden diese vervielfältigt und an die anderen Gruppen weitergegeben. Diese sollen die Infoblätter der anderen Teams mit Hilfe des Arbeitsblattes 18 nach verschiedenen Kriterien beurteilen. Die Ergebnisse werden miteinander verglichen und gemeinsam diskutiert.

Tipp – Vertiefung der zielgruppenadäquaten Aufbereitung von Inhalten:
Geben Sie Ihren SchülerInnen die Aufgabe, ihr Infoblatt für eine andere Zielgruppe, z.B. Kinder bis 10, Eltern von SchülerInnen der 5. bis 6. Schulstufe, umzugestalten. Diskutieren Sie anschließend, welche Probleme sich den SchülerInnen bei der Umgestaltung der Infoblätter gestellt haben und worin die konkreten Unterschiede in der Aufbereitung liegen.

Tipp – Abtestung der Infoblätter bei der Zielgruppe:

Führen Sie mit Ihren SchülerInnen gemeinsam einen Praxistest der erarbeiteten Infoblätter durch. Zu diesem Zweck kann Kontakt zum nächsten Seniorenwohnheim oder Pensionistenclub aufgenommen werden. Natürlich können auch Verwandte und Freunde der SchülerInnen, die dem Zielgruppensegment entsprechen, in den Praxistest mit einbezogen werden.

Die Testpersonen erhalten die Infoblätter und sollen diese entweder auf Basis des Arbeitsblattes 18 oder auf Basis eines kurzen Fragebogens, den die SchülerInnen selbst erstellen, bewerten.

Die Ergebnisse dieses Praxistests können anschließend gemeinsam ausgewertet und diskutiert werden und dienen als Basis für eine nochmalige Überarbeitung der Infoblätter.

Getroffen?

Arbeitsblatt 18,
Seite 168-169

Hit the nail on the head?

Arbeitsblatt 18,
Seite 170-171

**Infoblatt 2: Schutzschild aktiv?/Mobile phone security****Arbeitsblatt 18: Getroffen?/Hit the nail on the head?***Zusatzinformationen:*

Einer Umfrage der Forsa - Gesellschaft für Sozialforschung und statistische Analyse zur Handynutzung bei der Generation 65+ in Deutschland brachte im Mai 2011 folgendes Ergebnis:

Defizite normaler Handys

- zu viele überflüssige Funktionen (71%)
- zu wenig Wissen über Handys (52%)
- zu kleine Tasten (46%)
- zu komplizierte Bedienung (45%)

Vorteile von Seniorenhandys

- Die Notruffunktionen sind interessant. (77%)
- Handy macht das Leben angenehmer und leichter. (73%)
- Angehörige haben sichereres Gefühl durch die Erreichbarkeit. (72%)

Linkliste zu den Quellen von Infoblatt 2:

- **W-LAN**

- <http://wirtschaftsblatt.at/archiv/aktuell/1216217/print.do>: Artikel aus dem Wirtschaftsblatt über die Risiken von öffentlichen W-LAN-Netzen
- www.handysektor.de/index.php/a_bis_z/page/boese_zwillinge_evil_twins: Definition des Risikos „Böser Zwilling“
- www.pcwelt.de/tipps/Jedes-WLAN-sicher-nutzen-WLAN-Verbindung-auf-Smartphones-absichern-4702884.html: Artikel über technische Möglichkeiten, W-LAN-Netze sicher zu machen

- **Apps**

- www.handytarife.de/index.php?aid=2356: ausführlicher Artikel über Definition, Entstehung und Risiken von Apps
- <http://handywissen.at/was-koennen-handys/#c520>: Tipps zum sicheren Umgang mit Apps



- **Schadprogramme**

- www.handytarife.de/index.php?aid=1929: ausführlicher Artikel über die verschiedenen Ausformungen und die Verbreitung von Schadprogrammen sowie Sicherheitstipps
- www.computerbetrug.de/telefonabzocke/handy-viren-und-handy-dialer: ausführlicher Artikel über die verschiedenen Ausformungen und die Verbreitung von Schadprogrammen sowie Sicherheitstipps

- **Bluetooth**

- <http://handywissen.at/was-koennen-handys/#c302>: Funktionsweise von Bluetooth und Infrarotschnittstellen
- www.handysektor.de/index.php/aktuelles/netzwerk_more/immer_mehr_handys_machen_blaue: Funktionsweise von Bluetooth und Sicherheitstipps

Hauptteil E

Aufbau der Unterrichtseinheit	Materialien
<p>E ABSCHIED VOM HANDY Weitergabe, Entsorgung, Verkauf, Verlust, Diebstahl</p> <p>Verhalten bei Weitergabe und Entsorgung des Handys Arbeitsblatt 19 widmet sich dem richtigen Verhalten bei der Weitergabe oder Entsorgung eines Handys. Overheadfolie 9 bzw. 10 liefert die Lösung.</p> <p>Verhalten bei Verlust oder Diebstahl des Handys Arbeitsblatt 20 liefert die wichtigsten Informationen für den Fall des Handyverlustes oder -diebstahls.</p> <p>Abschließend wird gemeinsam besprochen, was die SchülerInnen vorbeugend tun können, um die Folgen eines unerwünschten Handyverlustes möglichst gering zu halten.</p>	<p>Ausradiert und für immer gelöscht Arbeitsblatt 19, Seite 172 Overheadfolie 9, Seite 173</p> <p>Erased and deleted forever? Arbeitsblatt 19, Seite 174  Overheadfolie 10, Seite 175</p> <p>Hilfe: Mein Handy ist weg! Arbeitsblatt 20, Seite 176</p> <p>Help! My mobile phone is gone! Arbeitsblatt 20, Seite 177 </p>

Arbeitsblatt 19: Ausradiert und für immer gelöscht?/Erased and deleted forever?

Zusatzinformationen:

Um Daten auf einem Handy endgültig und nicht wiederherstellbar zu löschen, gibt es je nach Handyhersteller bzw. Betriebssystem verschiedene Möglichkeiten. Um sicherzustellen, dass Daten nach dem Löschen tatsächlich vom System entfernt wurden und nicht wieder herstellbar sind, sollte man sich daher unbedingt im Handy-Handbuch über die geeignete Methode informieren.

Viele Handys bieten die Möglichkeit der Rückstellung des Handys auf die Werkseinstellungen – wird diese Option gewählt, so werden alle benutzerdefinierten Daten vom Handy gelöscht.

Weiterführender Link:

- www.chip.de/news/Apple-iPhone-Daten-sicher-loeschen_48075121.html: Handydaten sicher löschen, alle Betriebssysteme und Handyhersteller

Arbeitsblatt 20: Hilfe: Mein Handy ist weg!/Help! My mobile phone is gone!

Neben Präventivmaßnahmen sollten für den Fall der Fälle vorsorglich folgende Maßnahmen getroffen werden:

- Notieren der SIM-Karten-Nummer sowie der IMEI-Nummer und Aufbewahrung der Kennziffern unabhängig vom Handy
- regelmäßige externe Sicherung aller auf dem Mobiltelefon gespeicherten Daten
- so vorhanden: Aktivierung der automatischen Tastensperre mit PIN-Sicherung → nach kurzer Ruhezeit wird das Handy automatisch gesperrt, eine Weiterverwendung ist erst nach Eingabe des PINs möglich
- Aktivierung der Sperrfunktion des Telefons im Fall des Abschaltens bzw. des Einlegens einer fremden SIM-Karte → eine Weiterverwendung des Handys ist erst nach Eingabe einer von der HandybesitzerIn festgelegten Geheimnummer möglich

Zusatzinformation:

- **SIM-Karte**

Der Begriff „SIM“ ist die Abkürzung von „Subscriber Identity Module“, auf Deutsch „Teilnehmer-Identitätsmodul“.

Jede SIM-Karte enthält einen Speicherchip mit allen für die Mobilfunknutzung und zur Identifikation notwendigen Daten und Informationen, zusätzlich dazu gibt es Speicherbereiche, die vom Handyuser genutzt und beschrieben werden können.

Wird eine aktivierte SIM-Karte ins Handy eingelegt und dieses eingeschaltet, so erkennt das Handy dank der Informationen auf dem Speicherchip den Mobilfunkbetreiber und die aktuelle Funkzelle, in der es sich befindet.

Nicht nur das Handy, auch die SIM-Karte ist aufgrund der vielen Lese- und Schreibvorgänge, denen sie unterliegt, ein Verschleißteil.

- **IMEI-Nummer**

IMEI ist die Abkürzung von „International Mobile Equipment Identifier“. Es handelt sich dabei um eine 15-stellige Seriennummer, die jeweils nur einmal vergeben wird und somit jedes Handy eindeutig identifizierbar macht.

Es besteht sogar die Möglichkeit, Handys, sobald sie im Mobilfunknetz eingebucht sind, unabhängig von ihrer SIM-Karte nur auf Basis der IMEI-Nummer zu orten und zu sperren. In einigen Ländern, wie etwa Großbritannien, wird dies bereits durchgeführt, in Österreich ist dies noch nicht der Fall.




- **Fernzugriff aufs Handy**

Mittlerweile werden Softwarelösungen angeboten, mit deren Hilfe es möglich ist, via Online-Befehl oder SMS-Nachricht auf dem Handy gespeicherte Daten zu löschen. Diese Techniken sind allerdings nur bei GPS-Handys anwendbar.

Linksammlung:

- www.environmental-studies.de/SIM-Karte/sim-karte.html: Wissenswertes zur SIM-Karte
- www.handyortung.info/handydiebstahl/handydaten-loeschen-nach-diebstahl: Infos zum Löschen von Handydaten nach einem Diebstahl
- www.bmi.gv.at/cms/BK/praevention_neu/vermoegen/Handydiebstahl.aspx: Infoseite des Bundeskriminalamts mit Tipps zur Prävention, Handlungsanleitung im Falle eines Diebstahls sowie aktuellen Servicetelefonnummern der Mobilfunkbetreiber
- <http://handywissen.at/notfaelle>: Tipps für den Fall des Handyverlustes oder -diebstahls

Abschluss der Unterrichtseinheit

Aufbau der Unterrichtseinheit	Materialien
<p>Variante 1 – Kreuzwörterrätsel</p> <p>Wesentliche Informationen zum Thema werden in Form eines Kreuzwörterrätsels nochmals abgefragt und wiederholt.</p> <p>Variante 2 – Verfassen von Kurzanleitungen</p> <p>Die SchülerInnen erhalten die Aufgabe, zu den Fallbeispielen der Einstiegsvariante 1 Tipps zu verfassen, wie man die geschilderten Gefahrenquellen verhindern kann.</p> <p>Variante 3 – abschließender Ausblick</p> <p>Auf Arbeitsblatt 23 wird in zwei Interviews die „Post-Privacy-These“ behandelt. Diese in Deutschland entstandene These widmet sich der Annahme, dass wir in unserer vernetzten Welt keinen Anspruch mehr auf Datenschutz erheben können.</p> <p>Nachdem die SchülerInnen die zwei Artikel gelesen haben, werden folgende Fragen im Klassenverband diskutiert</p> <ul style="list-style-type: none"> ● Welchen Argumenten stimmen die SchülerInnen zu, welchen nicht? ● Wie argumentieren sie ihre Entscheidung? ● Gibt es Daten, die die SchülerInnen schützenswert finden? Wenn ja – welche sind das und warum sollten diese geschützt werden? <p>Variante 4 – Quiz</p> <p>Das Quiz ermöglicht eine lebendige Wiederholung der Sachinformationen zum Thema. Erklärende Antworten auf der Rückseite der Quizkarten gewährleisten bei Nicht-Wissen verstehendes Lernen und geben gleichzeitig die Möglichkeit, noch weitere Informationen zum Thema zu erhalten.</p> <p>Anhang - Vokabelliste</p>	<p>Alles klar?</p> <p>Arbeitsblatt 21, Seite 178-179 Overheadfolie 10, Seite 180</p> <p>Smart & safe? </p> <p>Arbeitsblatt 21, Seite 181-182 Overheadfolie 11, Seite 183</p> <p>Be smart!</p> <p>Arbeitsblatt 22, Seite 184-186</p> <p>Be smart! </p> <p>Arbeitsblatt 22, Seite 187-189</p> <p>Post-Privacy</p> <p>Arbeitsblatt 23, Seite 190-194</p> <p>Quiz</p> <p>Quizkarten</p> <p>Quiz </p> <p>Quizkarten</p> <p>Vokabelliste, Seite 195-196</p>

Arbeitsblatt 23: Post-Privacy

Zusatzinformationen:

Der Begriff „Post-Privacy“ ist um das Jahr 2009 im Zusammenhang mit einer Debatte ums Internet entstanden und bezeichnet einen Zustand, in dem es keine Privatsphäre mehr gibt und Datenschutz nicht mehr greift. Die Debatte drehte sich um die Frage, ob man angesichts der großen Mengen privater Daten im Internet in Sachen „Datenschutz“ resignieren oder die Datenmenge als Chance sehen soll.

Links & Quellen zum Thema:

- <http://de.wikipedia.org/wiki/Post-Privacy> : Wikipedia Eintrag zu „Post-Privacy“
- www.youtube.com/watch?v=p3ZEfl4owuY: Diskussion zu Post-Privacy, deutsche Teilnehmer: Christian Heller, Thilo Weichert
- www.youtube.com/watch?v=Z2dzLT3tvev: Diskussion zu „Digitales Leben 2.0 - Fluch oder Segen?“