Text

Description automatically generated with medium confidence

CSI-COP MOOC:

Ihr Recht auf Datenschutz im Internet

Inhalt

CSI-COP MOOC – informeller Bildungskurs Seite 1

Kursdetails Seite 3

Schritt 1: Datenschutz Seite 5

Schritt 2: Daten Seite 9

Schritt 3: Online-Tracking Seite 13

Schritt 4: Rechte auf Datenschutz und Privatsphäre Seite 20

Schritt 5: Tools zum Schutz Ihrer Daten und Privatsphäre Seite 24

Ihr Feedback zum Kurs Seite 29

Bewertung Ihres Lernens Seite 30

CSI-COP Citizen Scientist werden Seite 31

Umfrage Seite 32

**MOOC**

Der kostenlose informelle Kurzlehrgang von CSI-COP (Massiven offenen Online-Kurs – MOOC) kann online belegt oder als Dokument heruntergeladen werden. Der MOOC dauert zwischen 2½ bis 3 Stunden.

Beim MOOC geht es um Ihre Daten und Ihr Recht auf Privatsphäre im Internet. Im Internet werden Daten durch digitale Technologien in Websites und in Apps (Softwareprogramme auf mobilen Geräten) gesammelt. Zu diesen Technologien gehören Cookies, kleine Textdateien, die auf Desktop-Computern, Laptops oder Smart-Geräten (Tablets, Mobiltelefone) gespeichert werden, wenn Sie eine Seite im Internet besuchen. Cookies können digitale Tracker enthalten, wie z. B. das Verfolgen des genauen Standorts Ihres Geräts. App-Einstellungen können Berechtigungen für den Zugriff auf Ihre Kontakte, Ihre Kamera, Ihre Nachrichten, Ihr Mikrofon und andere Daten auf Ihren Mobilgeräten haben. Der Standort eines Geräts kann eine Person, die das Gerät verwendet oder besitzt, persönlich identifizieren, und hat somit Auswirkungen auf den Datenschutz und die Privatsphäre.

Das Hauptziel des von [CSI-COP](https://csi-cop.eu/) [EU Horizon 2020](https://cordis.europa.eu/project/id/873169) finanzierten Projekts ist es, die breite Öffentlichkeit allgemeinverständlich über Online-Tracking-Technologien und deren Deaktivierung aufzuklären. Dies ermöglicht es der breiten Öffentlichkeit, „Citizen Scientists“ zu werden. Ein Citizen Scientist (CS) ist ein Mitglied der breiten Öffentlichkeit, dass sich mit der Sammlung und Analyse von Daten im Rahmen eines Kooperationsprojekts mit professionellen Wissenschaftlern beschäftigt. Das Ziel von CSI-COP ist es, Citizen Scientists dazu zu bringen, **sich dem CSI-COP-Projektteam anzuschließen**, um zu untersuchen, inwieweit das Tracking standardmäßig im gesamten Internet erfolgt. Die Datenschutz-Grundverordnung (**DSGVO**) 2018 bietet eine Checkliste, anhand derer die Einhaltung beurteilt werden kann. Das CSI-COP-Team ist der Ansicht, dass der Citizen Science-Ansatz notwendig ist, um die Zusammenarbeit zwischen Bürgern und Wissenschaftlern zu fördern. Er soll untersuchen, inwieweit unsere Daten online über die von uns besuchten Websites und die von uns verwendeten Apps verfolgt werden.

Für wen ist dieser Kurs?

Dieser Kurs richtet sich an alle Personen ab 18 Jahren, die daran interessiert sind, zu verstehen, wie unsere Daten im Web und über von uns verwendete Apps erfasst werden, und die mehr darüber erfahren möchten, wie wir unsere Privatsphäre online schützen können.

Was Sie für diesen Kurs benötigen

Sie benötigen ein Smartphone, Tablet, Laptop oder Computer mit Internetzugang. Wenn Sie sich an einer Universität befinden oder eine lokale Bibliothek nutzen, können Sie möglicherweise auch auf kostenloses WLAN zugreifen. Beachten Sie jedoch, dass der Vorteil des kostenlosen öffentlichen WLANs mit der Gefahr verbunden ist, dass Hacker auf Ihre Daten zugreifen. Informationen zur Vermeidung von Risiken im öffentlichen WLAN finden Sie bei Kaspersky hier: <https://bit.ly/3v6thff>

Wenn Sie Twitter verwenden

Wir haben am Ende jedes Schritts einen kurzen Tweet vorgeschlagen, den Sie an andere senden können, um sie darüber zu informieren, dass Sie den informellen Bildungskurs von CSI-COP besuchen. Sie können CSI-COP markieren, indem Sie [@cop\_csi](https://twitter.com/cop_csi?lang=de) verwenden.

**Bitte überprüfen Sie die Kursdetails auf Seite 3, dann probieren Sie die informellen Lernschritte 1, 2, 3, 4 & 5 ab Seite 4 aus.** In jedem Schritt werden die Lernergebnisse und die Inhalte kurz vorgestellt. Für Hintergrundinformationen werden in jedem Schritt die Namen von Personen mit Links zu weiterführenden Informationen versehen. Weitere Details finden Sie am Ende des Schrittes in einem Abschnitt zum Weiterlesen.

Um Ihr Lernen und Ihr Verständnis zu verbessern, achten Sie bitte in jedem Schritt auf eine **große Frag**e. Dies fordert Sie auf, eine Frage zu einem Thema zu prüfen, bevor Sie etwas darüber erfahren. Sie können die „großen“ und andere Fragen mit Familie und Freunden diskutieren oder sich mit anderen in einem [Forum](https://csi-cop.eu/forum/) auf der CSI-COP-Website austauschen, Sie müssen sich zuerst unter diesem Link registrieren: <https://csi-cop.eu/citizenscientistlogin/>

Nach jedem Schritt haben Sie die Möglichkeit, Ihr Gelerntes zu überprüfen, und es werden Aktivitäten angeboten, die Ihnen hierbei helfen.

Nach dem letzten Schritt finden Sie einen Rückblick, um den gesamten Kurs zu überprüfen. Am Ende, nach Schritt 5, finden Sie auch Informationen darüber, wie Sie dem CSI-COP-Team beitreten können, um Citizen Scientists zu werden, die den Online-Datenschutz untersuchen, und ein Datenschutz-Champion werden.

Wir wünschen Ihnen viel Freude dabei!

**KURSDETAILS**

|  |  |
| --- | --- |
| **CSI-COP MOOC: ein Selbststudium der informellen Bildung** | *Ihr Recht auf Datenschutz im Internet* |
| **Ziele des MOOC** | Der kostenlose Online-Kurs von CSI-COP umfasst fünf Schritte. Wenn Sie jeden Schritt abschließen, erhalten Sie das Wissen, um fundierte Entscheidungen über Ihr Recht auf Online-Privatsphäre zu treffen, und erhalten die erforderlichen Fähigkeiten, um Tracking-Technologien im Internet und in Apps auf Ihren Android-Geräten (z.B., oder Tablet). Nach Abschluss können Sie ein informelles CSI-COP-Ausbildungszertifikat anfordern. Sie können dann von einem informellen Lernenden zu einem freiwilligen Citizen Scientist werden, der dem CSI-COP-Team beitritt, um zu untersuchen, inwieweit Ihre Daten über das Internet verfolgt werden (siehe Schritt 5).  <https://cordis.europa.eu/project/id/873169> |
| **Was Sie lernen werden**  *(Lernziele)* | 1) Gewinnen Sie Wissen über die Privatsphäre, die im Rahmen der Menschenrechtscharta gewährt wird  2) Praktische Fähigkeiten (Know-how) zum Aufdecken von Online-Tracking-Technologien, die in Websites und in Android-Apps eingebettet sind  3) Entdecken Sie, wie Sie Citizen Scientist werden und treten Sie dem CSI-COP-Team bei, um das Ausmaß des Online-Trackings durch digitale Tracking-Technologien zu untersuchen |
| **Kursdauer** | Dieser Kurs ist so konzipiert, dass er auf folgende Weise abgeschlossen wird:   * Alle fünf Schritte in einer Sitzung, einschließlich des informellen Lernens und der Aktivitäten, in 2½ -3 Stunden * In Ihrem eigenen Tempo. |
| **Details zur informellen Bildung** | |
| **Titel** | *Schutz Ihrer Daten* |
| **Ziele & Zusammenfassung** | Dieser Workshop ist so konzipiert, dass er an einem halben Tag in einer Sitzung absolviert wird. Sie können die Lernschritte jedoch an Ihre Verfügbarkeit anpassen.  In diesem Online-Workshop erhalten Sie ein umfassendes Verständnis der verschiedenen Aspekte des Datenschutzes und der Art und Weise, wie Ihre personenbezogenen Daten von Dritten bei Ihrer Online-Interaktion auf Websites und bei der Nutzung von Apps verwendet werden können. Sie erfahren, wie Sie fundierte Entscheidungen über Ihre personenbezogenen Daten treffen und wie Sie die Transparenz bei der Erhebung von Daten über Sie überprüfen können. |
| **Was Sie lernen werden -** *(Lernergebnisse)* | **Angestrebte Lernergebnisse des Kurses**  1. Beschreiben und diskutieren Sie die verschiedenen Aspekte des Datenschutzes.  2. Identifizieren und bewerten Sie die Art und Weise, wie personenbezogene Daten beim Surfen im Internet und der Nutzung von Apps auf Smart-Geräten erfasst werden.  3. Verstehen Sie die Rechte auf Privatsphäre, die sich aus Chartas zum Schutz unserer Daten ergeben |
| **Kursinhalt** | • Datenschutz und seine verschiedenen Aspekte  • Was sind personenbezogene Daten?  • Wie werden personenbezogene Daten durch unsere Internetnutzung erhoben?  • Rechte auf Privatsphäre (UN; EU; DSGVO)  • Online-Schutz Ihrer Daten. |

**SCHRITT 1**

|  |  |
| --- | --- |
| **Schritt 1 Titel:** | Verschiedene Aspekte der Privatsphäre |
| **Schritt Lernergebnis** | 1: Beschreiben und diskutieren Sie die verschiedenen Aspekte der Privatsphäre. |
| **Thema** | Datenschutz und seine verschiedenen Aspekte |
| **Große Frage** | Hat das Privatsphäre-Pferd geschraubt?  Fragen Sie Ihre Familie und Freunde, was sie über Privatsphäre denken. Sie können Ihre Ansichten im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen: <https://csi-cop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Jan Holvast (2009) „Diskussionen über Datenschutzfragen sind so alt wie die Menschheit“.  [Bitte lesen Sie den Abschnitt zum Weiterlesen am Ende von Schritt 1] |
| **Lerninhalte** | **Kurze Geschichte von „Privatsphäre“**  Laut Jan Holvast (2009) „Die Diskussion über Datenschutzfragen ist so alt wie die Menschheit. Angefangen mit dem Schutz des eigenen Körpers und des Hauses, entwickelte sich dies bald in Richtung der Kontrolle der persönlichen Daten.“  Im Jahr 1890 schrieb Warren & Brandeis „Dass der Einzelne vollen Schutz in Person und Eigentum genießen soll, ist ein Grundsatz, der so alt ist wie das Common Law“, und „in sehr frühen Zeiten bot das Gesetz nur bei körperlichen Eingriffen ein Leben lang Abhilfe und“ Eigentum". Sie fügten hinzu, dass „jetzt [im Jahr 1890] das Recht auf Leben … das Recht, in Ruhe gelassen zu werden“ bedeutet und „der Begriff ‚Eigentum‘ mittlerweile jede Form von Besitz umfasst – sowohl immaterieller als auch materieller Art“.  2011 informierte Nissenbaum: „Das Jahr 2010 war ein großes Jahr für den Online-Datenschutz. Berichte über Datenschutzfehler, wie sie beispielsweise im Zusammenhang mit Google Buzz und den launischen Datenschutzrichtlinien von Facebook standen, zierten die Titelseiten prominenter Nachrichtenmedien. In seiner Reihe „On What They Know“ richtete das Wall Street Journal ein Schlaglicht auf die zügellose Verfolgung von Personen aus verhaltensorientierten Werbegründen und aus anderen Gründen.“  In Bezug auf die Ethik der Privatsphäre konzentriert sich Marijn Sax (2018) „auf Fragen wie ‚Was ist der Wert der Privatsphäre?‘ und ‚Welche Datenschutznormen sollten von Einzelpersonen (einschließlich uns selbst), der Gesellschaft und dem Staat respektiert werden?‘  **Google Chrome**  Einige von Ihnen verwenden möglicherweise den Inkognito-Modus des Chrome-Browsers von Google, um Ihre Privatsphäre zu wahren. Es scheint jedoch, dass Google „heimlich Internetdaten sammelt, selbst wenn Benutzer im „Inkognito“-Modus surfen, um ihre Suchaktivitäten privat zu halten“. (Nayak und Rosenblatt, 2021). Eine Bloomberg-Nachrichtenmeldung 2021 berichtet, dass „Verbraucher einen Fall als „Sammelklage“ eingereicht haben, in der behauptet wird, dass „selbst, wenn sie die Datenerfassung in Chrome deaktivieren, andere von Websites verwendete Google-Tools am Ende ihre persönlichen Daten sammeln“ (Nayak und Rosenblatt, 2021). Weitere Informationen zu diesem Fall finden Sie auf Bloombergs neue Website hier: <https://bloom.bg/3gFt4vV>  **Facebook 533 Millionen Datenschutzverletzung**  Sie haben vielleicht die jüngsten Nachrichten gehört, dass wir, egal wie sehr wir versuchen, unsere Informationen einigermaßen geheim zu halten, bei der Nutzung sozialer Medien zur Verfügung des Plattformbesitzers stehen und unsere Kompetenz zum Schutz unserer Privatsphäre haben. Die persönlichen Daten von mehr als 530 Millionen Facebook-Nutzern waren im April 2021 auf einer Website für Hacker verfügbar (Holroyd, 2021). Zu den personenbezogenen Daten der 533 Millionen zählen Facebook-Nutzer in diesen Ländern:  - Mehr als 35 Millionen in Italien  - Über 32 Millionen in den USA  - Fast 20 Millionen Konten in Frankreich  - 11 Millionen Nutzer in Großbritannien und  - 6 Millionen Nutzer in Indien.  Lomas (2021) berichtet, dass der Datendump der Informationen, die Facebook-Nutzer auf dieser Plattform geteilt haben, Folgendes umfasst:  - Facebook-IDs  - Ganze Namen  - Telefonnummern  - Standorte  - Geburtsdaten  - Bios und  - Einige E-Mail-Adressen  Sie können mehr auf [TechCrunch](https://techcrunch.com/2021/04/06/answers-being-sought-from-facebook-over-latest-data-breach/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMUOIlLG_dSDm7w74IG-14xWYBlW6py7Mv17hgb8XiPn2uZ7Dkrhgu4A0krDDh0ttvoqMkev6D_h7Man-RtR7mMGNmk5i1_oayagVtIi3W8g3McHb1cTXnWDGzLr9fUa3u1DIYa3yMFn1UCx2zMqgcF9J0G_2nP_mU6aSU41mLXG&guccounter=2) lesen.  Wenn Sie ein Facebook-Nutzer sind und herausfinden möchten, ob Ihre Daten von dieser Facebook-Datenverletzung betroffen sind, können Sie dies entweder per E-Mail oder mit Ihrer Facebook-ID oder Telefonnummer auf diesen Websites überprüfen:  - Wurde ich gepwned? Hier: <https://haveibeenpwned.com/>  - Wurde ich geZucked? Hier: <https://haveibeenzucked.com/>  Sie können auch die Tweets von The Real Facebook Oversight Board „Holding Facebook to Account“ auf Twitter hier verfolgen: <https://twitter.com/FBoversight> |

|  |  |
| --- | --- |
|  | Worauf Sie sich in den nächsten Schritten freuen können  Im folgenden Schritt (Schritt 2) beginnen wir mit der Suche nach Daten und personenbezogenen Daten.  In Schritt 3 werden wir uns ansehen, *wie unsere Daten nachverfolgt werden*.  In Schritt 4 werden wir uns ansehen, *welche Rechte wir an unserer Privatsphäre haben*  Im letzten Schritt dieses Kurses, Schritt 5, lernen wir Online-Tools kennen, mit denen wir unsere Privatsphäre besser *schützen und unsere Daten schützen können.*  Überprüfen Sie Ihr Lernen  Bitte wiederholen Sie das, was Sie in Schritt 1 gelernt haben, mit einer Frage und zwei Aktivitäten als nächstes. |
| **Überprüfen Sie Ihr Lernen** | Was ist *Privatsphäre*? |
| **Aktivitäten** | **Aktivität 1**  Ist die folgende Aussage richtig oder falsch?  „Die Diskussion um den Datenschutz ist neu, seit der Erfindung von Facebook“.  **Aktivität 2:**  Besprechen Sie das Konzept der Privatsphäre mit Ihrer Familie, Freunden, Nachbarn oder Kollegen.  Was haben Sie über Ihr eigenes Verständnis von Datenschutz und die Sichtweise anderer auf Datenschutz erfahren?  Zur Erinnerung: Sie können Ihre Ansichten im CSI-COP-Website-Forum hier posten: https://csi-cop.eu/forum/ - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen:<https://csi-cop.eu/citizenscientistlogin/> |
| **Aktivitätszweck** | Gewinnen Sie Verständnis für Aspekte des Datenschutzes. |
| **Kurzer Tweet** | Sollte Komfort im Zeitalter des mobilen Zugangs zum Internet wichtiger sein als die Privatsphäre? |

|  |  |
| --- | --- |
| **Weiterführende Literatur für Schritt 1** | Links zum Weiterlesen, die in Schritt 1 erwähnt wurden, finden Sie, indem Sie den unterstrichenen Text unten auswählen:  **Empfohlen**  Lomas, N. (2021). *Von Facebook werden Antworten auf die neueste Datenpanne gesucht.* Tech Crunch. Von hier aus erreichbar: <https://tcrn.ch/3xfrTsE>  Nayak, M. und Rosenblatt, J. (2021). *Google muss sich beim Snooping beim "Inkognito"-Browsen dem Anzug stellen* Bloomberg-Technologie. Von hier aus erreichbar: <https://bloom.bg/3gFt4vV>  Der Twitter-Account des Real Facebook Oversight Board @FBoversight ist hier zugänglich: <https://twitter.com/FBoversight>  **Zusätzlich**  Holroyd, M. (2021). *Irland leitet Datenschutzuntersuchung zu Facebook-Hack ein.* Euronews – Irland. Von hier aus erreichbar <https://bit.ly/3mOfIOM>  Holvast, J. (2009). *Geschichte der Privatsphäre*. In V. Matyáš et al. (Hrsg.): *The Future of Identity,* IFIP AICT 298, S. 13–42, 2009. IFIP International Federation for Information Processing 2009. Erhältlich bei ResearchGate: <https://www.researchgate.net/publication/225802214_History_of_Privacy>  Nissenbaum, H. (2011). *Ein kontextbezogener Ansatz für den Online-Datenschutz. Dædalus*, Journal of the American Academy of Arts & Sciences, Bd. 140, Nr. 4 (Herbst 2011), S. 32-48. Von hier aus zugänglich:  <https://www.amacad.org/publication/contextual-approach-privacy-online>  Sax, M. (2018). *Datenschutz aus ethischer Sicht.* Kapitel in B. Van der Sloot & A. De Groot (Hrsg.), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (S. 143-173). Amsterdam: Amsterdam University Press. Erreichbar über diesen Link: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299047>  Warren, S. D. & Brandeis, L.D. (1890). *Das Recht auf Privatsphäre*. Harvard Law Review, Bd. 4, Nr. 5. (15. Dezember 1890), S. 193-220. Zugänglich von: [Das Recht auf Privatsphäre bei JSTOR](https://www.jstor.org/stable/1321160?origin=crossref&seq=1#metadata_info_tab_contents) |

**SCHRITT 2**

|  |  |
| --- | --- |
| **Schritt 2 Titel:** | Daten und personenbezogene Daten |
| **Schritt Lernergebnis** | 1: Beschreiben und diskutieren Sie die verschiedenen Aspekte der Privatsphäre. |
| **Thema** | Was sind personenbezogene Daten? |
| **Große Frage** | *Warum sollte es mich interessieren, wer Zugriff auf meine Daten hat, ich habe nichts zu verbergen?*  Fragen Sie Ihre Familie und Freunde, was sie von ihren Daten halten. Sie können Ihre Ansichten im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen: <https://csicop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Andreas Weigend (2017): „Jedes Mal, wenn wir etwas googeln, jemanden Facebook, irgendwo Uber oder auch nur ein Licht anmachen, erzeugen wir Daten, die Unternehmen sammeln.“  [Bitte lesen Sie den Abschnitt zum Weiterlesen am Ende von Schritt 2] |
| **Lerninhalte** | **Was sind Daten?**  Zusammenfassung: In Schritt 1 wurden wir in das Konzept der „Datenschutz“ eingeführt.  In Schritt 2 des informellen Schulungskurses von CSI-COP werden Sie verstehen, „was Daten sind“ und „welche Daten über Sie“ an verschiedenen Aspekten Ihres Online-Lebens beteiligt sind: vom Online-Shopping über das Benachrichtigen von Freunden bis hin zur Suche nach Informationen.  Die Singularform ist „Daten“ ist Datum:  • ein einzelnes Stück *Qualität* oder *Quantität* über etwas  Daten sind der Plural (mehr als ein einzelnes Element):  • Informationspunkte, zum Beispiel Daten über Sie wie  Wenn Sie ein Student sind, egal ob Sie ein "Heimat" oder ein internationaler Student sind   * Geburtsdatum * Voraussetzungen für einen Studienplatz * Privatadresse, Semesteradresse * Kontakt Nummer   Daten sind überall und werden in vielen Formen gespeichert:   * *Unstrukturiert:*   Betrachten Sie YouTube-Videos  Instagram-Bilder untersuchen  E-Mails lesen  Satellitenbilder  Wetterdaten   * *Strukturiert:*   Studierenden-/Personalausweisnummer – Zahlenfolge  NHS- oder Sozialversicherungsnummer  Flugbuchungen  Von Irwin (2021): „Unter bestimmten Umständen kann jede der folgenden Personen als personenbezogene Daten angesehen werden:“:   * Ein Vor- und Nachname * Eine Heimatadresse * Eine E-Mail Adresse * Eine Ausweisnummer * Standortdaten * Eine Internet Protocol (IP)-Adresse * Die Werbekennung Ihres Telefons   **Personenbezogene Daten sind Daten, die eine „natürliche“ (lebende) Person identifizieren.**  Pat Walshe von **‚Privacy Matters**‘ sagt: „Wir nutzen unsere Smartphones und Computer wie nie zuvor, um Anrufe zu tätigen, persönliche Texte und Bilder zu senden, Menschen über die Dienste WhatsApp oder Snapchat Nachrichten zu senden, online Lebensmittel oder Medikamente einzukaufen, um persönliche Dinge aus unserem Leben zu teilen in sozialen Medien, nach Informationen zu psychischer oder physischer Gesundheit, Politik, Religion oder zu besuchenden Orten suchen, Websites durchsuchen, Feedback hinterlassen und unsere Vorlieben und Abneigungen angeben. Digital zu sein erzeugt eine Fülle von Daten über uns, die oft persönlich und sensibel sind. Daten, die uns möglicherweise besser kennen lassen, als wir uns selbst kennen“ ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  Wir können **freiwillig Daten angeben**, wenn wir eine Online-Bestellung aufgeben oder einen Gesundheitstermin buchen. Es können Daten über uns und unsere Geräte und unser Online-Verhalten **erfasst und beobachtet werden** (z. B. die von uns besuchten Websites, die von uns angehörten Lieder oder Filme, die wir verwenden, die Art des von uns verwendeten Geräts, unsere Standorte – ob wir es bemerken oder nicht). Aus der Profilerstellung und der Analyse von Informationen über uns können Daten **abgeleitet werden** (z. B. welcher Benutzername ein Lied gehört oder einen Film online angesehen hat, die Kategorie des Liedes oder Films, wann eine Person ein Lied oder einen Film pausiert hat, zusammen mit Datum und die Zeit, zu der sie pausierten und neu starteten oder das Hören oder Zuschauen aufhörten, der Standort, an dem sie sich befanden (zumindest das Land) – Daten, die wie ein digitaler Schatten von Online-Aktivitäten sind. ([Privacy Matters](https://twitter.com/privacymatters?lang=en))  Neben personenbezogenen Daten. Es gibt auch **sensible personenbezogene Daten**. Gemäß der Datenschutz-Grundverordnung (DSGVO), über die wir in Schritt 4 mehr erfahren werden, können **sensible personenbezogene Daten** im Sinne der DSGVO Daten umfassen, die Ihre:   * Volksgruppe oder ethnische Herkunft * religiöse Ansichten * politische Meinungen * Gewerkschaftsmitgliedschaften.   Zu den sensiblen personenbezogenen Daten zählen auch Daten über die Gesundheit einer Person (z. B. psychisch oder physisch); Daten über das Sexualleben oder die sexuelle Orientierung einer Person; genetische Daten; biometrische Daten (zur eindeutigen Identifizierung einer Person) und Daten zu strafrechtlichen Verurteilungen und Straftaten ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  Brodkin (2021) berichtete im April 2021, dass T-Mobile:  „… ein neues Programm starten, das einige Daten verwendet, die wir über Sie haben.“  „*einschließlich Informationen, die wir aus Ihren Web- und Gerätenutzungsdaten erfahren* (wie die auf Ihrem Gerät installierten Apps)“  „und Interaktionen mit unseren Produkten und Dienstleistungen für unsere eigene Werbung und Werbung von Drittanbietern, es sei denn, Sie sagen uns, dies nicht zu tun“.  Wie fühlen Sie sich, wenn Ihr Mobilfunkanbieter Ihnen mitteilt, dass er sich wie T-Mobile verhalten würde? Oder wenn Sie T-Mobile nutzen, wie stehen Sie zu deren Aussage zur Erhebung und Verwendung Ihrer Daten?  Worauf Sie sich in den nächsten Schritten freuen können  Im folgenden Schritt (Schritt 3) werden wir uns ansehen, wie unsere Daten nachverfolgt werden.  In Schritt 4 werden wir uns ansehen, welche Rechte wir an unserer Privatsphäre haben  Im letzten Schritt dieses Kurses, Schritt 5, lernen wir Online-Tools kennen, mit denen wir unsere Privatsphäre besser schützen und unsere Daten schützen können.  Überprüfen Sie Ihr Lernen  Bitte wiederholen Sie das, was Sie in Schritt 2 gelernt haben, mit einer Frage und zwei Aktivitäten als nächstes. |
| **Überprüfen Sie Ihr Lernen** | Was sind *personenbezogene Daten*? |
| **Aktivitäten** | **Aktivität 1: Kurztest**  Welche der folgenden Namen beziehen sich auf personenbezogene Daten?   * Leonardo da Vinci * Präsident Joe Biden * Freddie Mercury * Königin Elizabeth die zweite * Alan Turing * Meghan Markle * Albert Einstein * Der Papst * Kim Kardashian   Die Antwort auf Schritt 2 Aktivität 1 wird in Schritt 3 bereitgestellt.  **Aktivität 2**  Suchen Sie zum Beispiel nach TED-Vorträgen und sehen Sie sich diese an, Tech-Soziologe, Zeynap Tufekci TED Global NYC-Vortrag, September 2017:  „**Wir bauen eine Dystopie auf, nur um die Leute dazu zu bringen, auf Anzeigen zu klicken.“**  Zur Erinnerung: Sie können Ihre Ansichten zu Ihren Lernergebnissen im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen: <https://csi-cop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Verstehen Sie, was *personenbezogene Daten* sind. |
| **Lerninhalte** | Die Aussage: „Ich habe nichts zu verbergen, deshalb ist es mir egal, wer Zugriff auf meine Daten hat“ ist falsch |

|  |  |
| --- | --- |
| **Weiterführende Literatur für Schritt 2** | Links zum Weiterlesen, die in Schritt 2 erwähnt wurden, finden Sie, indem Sie den unterstrichenen Text unten auswählen:  **Empfohlen**  Brodkin, J. (2021). *T-Mobile verkauft Ihre Webnutzungsdaten an Werbetreibende, es sei denn, Sie widersprechen*. arsTECHNICA. Von hier aus erreichbar: <https://bit.ly/3sUdkaQ>  Irwin, L. (2021). *Persönliche Daten vs. sensible Daten: Was ist der Unterschied?* IT-Governance. Von hier aus erreichbar: <https://bit.ly/3vhoRlX>  Privacy Matters auf Twitter: @PrivacyMatters: <https://twitter.com/privacymatters?lang=de>  Buch, das möglicherweise in Ihrer örtlichen Bibliothek aufbewahrt wird  Weigend, A. (2017). *Daten für die Menschen: So können Sie unsere Post-Privacy-Economy für Sie arbeiten lassen*. Basic Books: New York |

**SCHRITT 3**

|  |  |
| --- | --- |
| **Schritt 3 Titel** | Online-Tracking-Technologien |
| **Schritt Lernergebnis** | 1: Beschreiben und diskutieren Sie die verschiedenen Aspekte der Privatsphäre.  2: Identifizieren und bewerten Sie die Art und Weise, wie personenbezogene Daten beim Surfen im Internet und der Nutzung von Apps auf Smart-Geräten erfasst werden |
| **Thema** | Wie werden bei unserer Internetnutzung personenbezogene Daten erhoben? |
| **Große Frage** | *Welchen Schaden können Online-Tracking-Technologien anrichten?*  Fragen Sie Ihre Familie und Freunde, was sie von ihren Daten halten. Sie können Ihre Ansichten im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen: <https://csicop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Nigel Warburton (2020): *„Ohne Ihre Erlaubnis … sammeln Technologieunternehmen Ihre Daten – Ihren Standort, Ihre Vorlieben, Ihre Gewohnheiten, Ihre Ängste, Ihre Krankheiten, Ihre Politik – und teilen sie untereinander.“*  [Bitte lesen Sie den Abschnitt weiterführende Literatur am Ende von Schritt 3] |
| **Lerninhalte** | **Wie Informationen über Sie im Internet gesammelt werden**  Um zusammenzufassen, was wir in den beiden vorherigen Schritten gelernt haben:   * In Schritt 1 wurden wir in das Konzept der „Datenschutz“ eingeführt. * In Schritt 2 haben wir erfahren, dass sich „personenbezogene Daten“ auf eine natürliche (lebende) Person beziehen   In diesem Schritt lernen wir die verschiedenen Online-Tools kennen, die bei der Nutzung des Internets Daten sammeln.  Produktmanagerin Eliza Crawford (2020) teilt uns mit, dass der Grund für die Erfassung von Daten über Sie im Internet darin besteht, zu erfahren, wie Sie sich beim Besuch einer Website verhalten. Dies dient dazu, *„Einblicke darüber zu gewinnen, wie … Kunden Websites nutzen, um ein personalisiertes Online-Erlebnis zu bieten und den Benutzer durch gezielte Werbung zu monetarisieren“*.  Crawford (2020) erklärt, warum Online-Tracking stattfindet:   * *„Wenn Sie bei Google nach einem Restaurant suchen und der Dienst Ihnen eine Liste mit Restaurants in Ihrer Nähe zur Verfügung stellt, liegt dies daran, dass die Suchmaschine Ihren Standort kennt.“* * *„Wenn ein E-Commerce-Shop Ihnen eine Liste empfohlener Produkte anzeigt, weiß er, was Ihnen gefällt, da er Artikel verfolgt, die Sie sich angesehen oder zuvor gekauft haben.“*   Pat Walshe (Privacy Matters) erinnert uns daran, dass **Verhaltensdaten** Folgendes umfassen können:   * Ihre **Webbrowserdaten** – die von Ihnen besuchten Websites, das Datum und die Uhrzeit Ihres Besuchs, das Land, aus dem Sie besucht haben (abgeleitet von Ihrer IP-Adresse – eine eindeutige Zeichenfolge, die jedes Gerät identifiziert, das sich mit dem Internet verbindet und das automatisch gesendet wird, wenn Sie eine Website besuchen). Bedenken Sie auch, dass sie beim Verlassen einer Website erkennen können, welche Website Sie als nächstes besuchen, und die nächste Website, die Sie besuchen, möglicherweise erkennen kann, von welcher Website Sie gekommen sind. All dies würde als Verhaltensdaten beim Surfen im Internet betrachtet werden. * **„Clickstream-Verhalten“** – Daten über die Interaktionen einer Person auf einer Website, einschließlich dessen, was sie anklickt und scrollt und auf einem Touchscreen tippt * **„Suchmaschinen“** wie Google, die möglicherweise Informationen darüber sammeln und verwenden, wonach Sie suchen, auf welche Ergebnisse Sie klicken, Ihre IP-Adresse und die möglicherweise eine eindeutige Cookie-Kennung verwenden, um Sie zu verfolgen. * **Standort** – der Ort und die Art des Ortes, den Sie besuchen (Supermarkt, Casino, Kultstätte, Krankenhaus), oder wo Sie eine App verwendet haben, Datum und Uhrzeit, gefahrene Route, Häufigkeit eines Besuchs oder die von Ihnen gefahrenen Routen. Standortdaten können sehr aufschlussreich und verhaltensbezogen sein. * **Kaufhistorie** – Dies kann Arten von Abonnements umfassen (Gewerkschaftsmitgliedschaft, Fitnessstudio, Zeitungen usw.), Hotel- oder Restaurantreservierungen, die möglicherweise über die Suche, Karten, intelligente Assistenten oder direkt von Einzelhändlern oder Drittanbieterdiensten usw. vorgenommen wurden. * **Zahlungs- oder „**[Transaktionsdaten](https://medium.com/the-capital/what-you-dont-know-about-transactional-privacy-but-you-should-d0072941d050)**“** – Zahlungen, aus denen hervorgeht, an wen/welche Organisation Sie bezahlt haben (die die Art der Organisation offenlegen können – Klinik, Apotheke, Alkoholanbieter, Lebensmitteleinzelhändler, Buchhändler usw.) und wie viel, wann und wie oft. Tap-and-Go-Kartenzahlungen sind ein gutes Beispiel – denken Sie an den Kaffee, den Sie zu Beginn einer Fahrt kaufen, an Ort, Datum und Uhrzeit, an dem Sie bezahlt haben, und dann an Zahlungen, die Sie später am Tag mit derselben Karte tätigen. * **Streaming-Medien** – „[Du bist, was du streamst](http://assets.ctfassets.net/ziwa9xqm84y1/CFPSdMWTrtrhdD8iVHIcy/b136bd5e622c52675ec7e0b7dbde4625/Spotify_Media_Kit_2018_-_CA.pdf)“ und „[Sie wissen, was du letzte Nacht gesehen hast](https://www.nytimes.com/2019/10/25/business/media/streaming-data-collection-privacy.html)“. Beim Streaming von Medien werden viele Verhaltensdaten generiert über:   + das Datum und die Uhrzeit, zu der Sie auf einen Musik-, Audio- oder TV-/Film-Streaming-Dienst zugegriffen haben und den nicht genauen Standort (Landes- oder Regionsebene), von dem aus Sie darauf zugegriffen haben   + welches Profil auf den Dienst zugegriffen und ihn verwendet hat (ein Name + Kategorie, z. B. Kind)   + die Kategorie Musik, Hörbuch, TV/Film (z.B. politischer Horror, Erwachsene)   + sucht nach Inhalten   + ob Sie einen Song oder Film pausiert haben und wie lange (einschließlich Datum(en) und Uhrzeit(en))   + ob Sie einen Song oder eine TV-Episode-Film-Audiospur übersprungen/aufgegeben haben   + ob Sie Inhalte geteilt haben und mit wem und Ihre Interaktionen mit anderen innerhalb des Dienstes   + ob Sie einen Song, eine Fernsehsendung oder einen Film bewertet haben   + von Ihnen erstellte Playlists oder „Watch“-Listen   + das Gerät, das für den Zugriff auf den Dienst verwendet wird, sowie die IP-Adresse und die Gerätekennungen * **Aktivitäts-/Gesundheitsdaten** – Daten über Ihre Nutzung von Aktivitäts-Apps wie Radfahren, Laufen, Gehen oder Daten über Ihre Gesundheit, wie sie über Ernährungs- oder Fruchtbarkeits-Apps erhalten werden. Diese Daten können sehr aufschlussreich sein und beispielsweise oft mit Ihrem Standort in Verbindung gebracht werden. * **Social-Media-Diagramm** – Daten, die miteinander verbundene soziale Beziehungen zwischen Menschen und ihre Art und ihre Kommunikationsmuster aufdecken   Eine Studie von Ghostery (2017)  *„hat ergeben, dass Tracker, die Daten zum Online-Verhalten von Internetnutzern sammeln, auf mindestens 79 Prozent der Websites (eindeutige Domains) weltweit vorhanden sind. Webtracking ist so weit verbreitet, dass etwa zehn Prozent der Websites die von ihnen gesammelten Daten an zehn oder mehr verschiedene Unternehmen senden (eindeutige Tracker-Domains). Beim Web-Traffic werden 15 Prozent aller Seitenaufrufe im Internet von zehn oder mehr Trackern überwacht. Am weitesten verbreitet sind der Studie zufolge Tracking-Skripte von Google (60,3 Prozent der Seitenaufrufe) und Facebook (27,1 Prozent)“.*  Dieses Tracking erfolgt über digitale Tools:  **Cookies:**  Cookies sind kleine Datenpakete, die Websites auf dem Gerät des Benutzers speichern. Websites **verwenden häufig Cookies, um sich an Benutzereinstellungen zu erinnern** und **ein personalisiertes Erlebnis zu bieten sowie um Informationen für Werbung zu gewinnen**. Sobald eine Website ein Cookie auf dem Computer eines Benutzers abgelegt hat, kann der Cookie-Anbieter weiterhin darauf zugreifen. Auf diese Weise können Websites Cookies verwenden, um Benutzer von Seite zu Seite oder von Seite zu Seite zu verfolgen. Wie lange ein Cookie einen Benutzer verfolgen kann, hängt von der Art des Cookies ab. Beispiel: Sitzungsbezogen, Dauerhaft, Erstanbieter; Drittanbieter (Crawford, 2020).  **Fingerabdruck:**  Fingerabdruck ist eine Form des Website-Trackings, **bei dem die Attribute des Geräts oder Browsers des Benutzers verwendet werden, um ein Profil eines Benutzers zu erstellen.** Zu den Informationen, die Fingerabdrucke verwenden, gehören Ihr Gerät, das Betriebssystem, das Sie auf dem Gerät verwenden, Bildschirmauflösung, Browser und Browserversion, Sprache und Zeitzone. Crawford (2020) stellt fest: „Für sich genommen ist nicht jede einzelne Information so wertvoll. Alles in allem bietet es jedoch eine unglaublich genaue Möglichkeit, Benutzer zu identifizieren. Die **Electronic Frontier Foundation** ([EFF](https://www.eff.org/)) betreibt eine Site ‚[Cover your tracks](https://coveryourtracks.eff.org/)‘, die Ihren Browser testet, um zu zeigen, wie einzigartig Ihr Fingerabdruck im Vergleich zu anderen ist, die die Site verfolgt hat.“  **E-Mail-Tracking:**  E-Mail-Tracking-**Software platziert ein unsichtbares Bildpixel in Ihren E-Mails, das die genaue Uhrzeit und das Datum erkennen kann, an dem Sie eine E-Mail geöffnet haben.** Der Grund für das E-Mail-Tracking ist, dass Unternehmen/Händler usw. Zeit sparen und erfahren, ob die erste E-Mail eines Unternehmens für Sie interessant genug war, um sie zu öffnen. Wenn nicht, ist es unwahrscheinlich, dass Sie zukünftige Folge-E-Mails öffnen. Durch die Vermeidung unnötiger Folge-E-Mails spart das E-Mail-Tracking Zeit sowohl für den Vertriebsmitarbeiter als auch für den E-Mail-Empfänger. Wenn ein Unternehmen bemerkt, dass ein Kontakt auf die gesendeten Links klickt und ein Anschreiben oder ein angehängtes Angebot anzeigt, weiß das Unternehmen, dass Sie derzeit im Kopf sind. Wenn Sie sich zu diesem Zeitpunkt an Sie wenden, wenn Sie über einen Vorschlag eines Unternehmens nachdenken, beispielsweise zum Kauf eines Kleidungsstücks, wird das Gespräch für das Unternehmen/den Einzelhändler viel relevanter und aktueller.  Die Studie von Sivan-Sevilla et al. (2020) ergab, dass *„Unternehmen, von denen wir vielleicht noch nie gehört haben, Datenpunkte zu jedem Aspekt unseres Lebens sammeln – unsere Interessen, Einkäufe, unseren Gesundheitszustand, Standorte und mehr“*.  IAB (2019, zitiert in Sivan-Sevilla et al., 2020)  *„Diese Datenpunkte werden dann zu außergewöhnlich aufschlussreichen Verhaltensprofilen kombiniert, die intime Teile unserer Identität enthüllen und die milliardenschwere Werbeindustrie antreiben, die behauptet, vorherzusagen, was wir wahrscheinlich konsumieren, um uns mit Anzeigen anzusprechen“.*  Sivan-Sevilla et al. (2020) berichten weiter, dass Werbetreibende, wenn sie Informationen über medizinische Probleme, Bildungsinteressen und Nachrichtenkonsumgewohnheiten der Benutzer austauschen, besser wissen, wann ein Benutzer in einen Verbraucher verwandelt werden kann Kaufentscheidungen, die Werbetreibende sonst nicht vorhersagen könnten. Studien haben gezeigt, wie Daten von verschiedenen Websites aggregiert und verwendet werden, um Rückschlüsse auf die Demografie und Interessen der Benutzer zu ziehen, wodurch sie manipulativen Praktiken ausgesetzt werden, die versuchen, sie zum „richtigen“ (personalisierten) Zeitpunkt zum Klicken auf die „richtige“ (personalisierte) Werbung zu bewegen … Die Werbeindustrie hatte diese Momente als **„primäre Verwundbarkeitsmomente der Verbraucher“** definiert … in denen die Nutzer „einzigartig empfänglich“ sind …“.  Srinivasan (2020) stellt klar, dass:  *„Der Aufstieg des elektronischen Anzeigenhandels, heute allgemein als „programmatische Werbung“ bekannt, ging parallel zum Aufstieg des elektronischen Handels in verschiedenen Wirtschaftssektoren…. Das frühe Werbetechnologieunternehmen* ***Right Media*** *hat die* ***RMX****-„Werbebörse“ eingeführt,* ***den ersten elektronischen Handelsplatz für Anzeigen****. ….. Heute betreibt ein einziges Unternehmen,* ***Google****, gleichzeitig die führende Börse sowie die führenden Zwischenhändler (d.h. Vermittler), die Publisher und Werbetreibende für den Handel nutzen müssen … Google verkauft nicht nur Werbeflächen von Websites Dritter, es verkauft Werbeflächen, die auf seinen eigenen Websites, der Google-Suche und YouTube erscheinen“.*  Srinivasan (2020) berichtet:  *„Das Werbegeschäft hat sich in den letzten zwei Jahrzehnten drastisch verändert. Heutzutage wird die größte Werbekategorie, die Online-Werbung, kaum noch von Menschen verhandelt. Fortschritte in der Technologie ermöglichen den elektronischen Kauf und Verkauf von Werbeflächen über zentralisierte Handelsplätze mit hoher Geschwindigkeit, ohne dass sich die Leute jemals von Angesicht zu Angesicht treffen müssen. Wenn ein Benutzer eine Website besucht, wird die Werbefläche auf einer Seite sofort an einen oder mehrere dieser Orte weitergeleitet. Dort wird der Platz in Echtzeit an den Meistbietenden versteigert. Nach Abschluss dieser Auktionen kehren die Anzeigen der Werbetreibenden zurück und werden dem Benutzer rechtzeitig zum Laden der Seite angezeigt, und bevor der Benutzer bemerkt, dass etwas passiert ist. Der Nutzer sieht nur auf ihn ausgerichtete Anzeigen, beispielsweise für die Barclays Bank.“*  Sie werden jetzt vielleicht verstehen, dass viele Daten zunehmend von Personen erfasst, beobachtet und abgeleitet werden, mit denen Sie eine direkte Beziehung haben, nicht nur, um grundlegende Dienste bereitzustellen, die Sie anfordern, sondern zunehmend, um „Erfahrungen zu personalisieren“, unabhängig davon, ob Sie dies wünschen oder nicht, und /oder um Sie mit Werbung auf und außerhalb ihrer Websites, Apps und Dienste anzusprechen. Ihre Daten werden jedoch nicht nur von Personen erfasst, beobachtet und abgeleitet, mit denen Sie eine direkte Beziehung haben, sondern auch von Dritten im Werbeökosystem, die möglicherweise in die von Ihnen besuchten Websites oder die von Ihnen verwendeten Apps eingebettet sind, um sie gezielt anzusprechen Sie zum Beispiel mit [verhaltensbasierter Werbung](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf). Ihre Daten können verwendet werden, um Ihnen im Web und in Apps für Behavioral-Targeting-Zwecke wie [Echtzeitgebote](https://www.outbrain.com/blog/programmatic-advertising/) zu folgen, die es Werbetreibenden ermöglichen, automatisch in Echtzeit zu bieten, um Personen basierend auf bestimmten Kriterien anzusprechen – z.B. einer bestimmten Altersgruppe und eines bestimmten Geschlechts oder Typs des Mobilgeräts oder Standorts.  Daten über SIE können also sehr persönlich sein und intime Aspekte Ihres Lebens offenbaren. Es kann sich auf eine Weise auswirken, die Sie nie in Betracht gezogen haben und die Ihre Erwartungen an den Datenschutz verletzt und Ihre Privatsphäre nicht respektiert und schützt. Beispielsweise [wurde festgestellt](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdfhttps:/fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf), dass die Grindr-App Informationen mit einer *„großen Anzahl von Dritten“* teilt, die an Profiling und Werbung beteiligt sind. Geteilte Daten *„einschließlich IP-Adresse, Werbe-ID, GPS-Standort, Alter und Geschlecht“.* Dies führte zu einer Untersuchung der norwegischen Datenschutzbehörde, die Grindr eine Geldstrafe von umgerechnet 8,6 Millionen Pfund (100 Millionen Kronen) [auferlegte](https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information).  Alle oben besprochenen Datentypen sind personenbezogene Daten, die durch Datenschutzgesetze wie die DSGVO und das elektronische Datenschutzgesetz der EU (die [ePrivacy-Richtlinie](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=EN)) geschützt sind. Wir werden im nächsten Schritt (Schritt 4) der CSI-COP's diskutieren informellen Lernkurs. Diese Gesetze erlegen privaten und öffentlichen Organisationen Verpflichtungen auf, die Daten über Sie erfassen, beobachten und ableiten und Rechte über diese Nutzung gewähren. Auch dies wird in Abschnitt 4 des Kurses besprochen.  Aber nehmen Sie sich einen Moment Zeit und überlegen Sie, was Ihre Daten über SIE und ANDERE aussagen, mit denen Sie verbunden sind.  Beachten Sie auch, dass Sie bei der Nutzung von „kostenlosem“ Wifi Informationen über Sie angeben müssen, um auf das Internet zugreifen zu können.  Worauf Sie sich in den nächsten Schritten freuen können  Im folgenden Schritt (Schritt 4) werden wir uns ansehen, welche *Rechte wir an unserer Privatsphäre haben.*  Im letzten Schritt dieses Kurses, Schritt 5, lernen wir Online-Tools kennen, mit denen wir unsere Privatsphäre besser *schützen und unsere Daten schützen können.*  Überprüfen Sie Ihr Lernen  Bitte wiederholen Sie, was Sie in Schritt 3 gelernt haben. Die Antwort auf Schritt 2-Aktivität 1 finden Sie mit zwei Aktivitäten für diesen Schritt. |
| **Überprüfen Sie Ihr Lernen** | Cookies  Fingerabdruck  E-Mail-Tracking |
| **Aktivitäten** | **Antwort auf Schritt 2 Aktivität 1**  In Aktivität 1 in Schritt 2 wurden Sie aufgefordert, personenbezogene Daten aus einer Namensliste zu ermitteln. Da sich personenbezogene Daten nur auf natürliche (lebende) Personen beziehen. Für die Personen in der Liste, die nicht mehr leben, sind ihre Namen keine personenbezogenen Daten. Hast du richtig geraten? Überprüfen Sie unten:   * Leonardo da Vinci – keine personenbezogenen Daten * Präsident Joe Biden * Freddie Mercury – keine personenbezogenen Daten * Königin Elizabeth die zweite * Alan Turing – keine personenbezogenen Daten * Meghan Markle * Albert Einstein – keine personenbezogenen Daten * Der Papst * Kim Kardashian   **Schritt 3 Aktivität 1**   1. Suchen Sie im Internet nach den verschiedenen Arten von Cookies, die in Websites eingebettet werden können 2. Was ist der Unterschied zwischen Fingerabdruck und E-Mail-Tracking?   **Schritt 3 Aktivität 2**  Besprechen Sie mit Familie, Freunden, Nachbarn oder Kollegen, was Sie unter ***„Online-Verhaltensprofilierung“*** verstehen und wie sie im Web betrieben wird.  Zur Erinnerung: Sie können Ihre Ansichten zu Ihren Lernergebnissen im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen: <https://csi-cop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Erfahren Sie mehr über die Erstellung von Online-Verhaltensprofilen. |
| **Lerninhalte** | Tracking-Technologien |

|  |  |
| --- | --- |
| **Weiterführende Literatur für Schritt 3** | Links zum Weiterlesen, die in Schritt 3 erwähnt wurden, finden Sie, indem Sie den unterstrichenen Text unten auswählen:  **Empfohlen**  Crawford, E. (2020). *Website-Tracking: Warum und wie verfolgen Websites Sie? CookiePro-Blog: Cookie-Compliance.* Von hier aus zugänglich: <https://www.cookiepro.com/blog/website-tracking/>  EFF (kein Datum). *Die Electronic Frontier Foundation. Die führende gemeinnützige Organisation, die die digitale Privatsphäre, Redefreiheit und Innovation [seit 30 Jahren verteidigt und zählt](https://www.eff.org/tags/eff30)!* Von hier aus erreichbar: <https://www.eff.org/>  Ghostery (2017). 79 *Prozent der Websites weltweit verfolgen heimlich Ihre personenbezogenen Daten*. Ghostery. Von hier aus erreichbar: <https://www.ghostery.com/press/ghostery-global-tracking-study/>  Privacy Matters auf Twitter: @PrivacyMatters: <https://twitter.com/privacymatters?lang=de>  **Weiterlesen**  Sivan-Sevilla, I., Chu, W., Liang, X. und Nissenbaum, H. (2020). *Unbegründete Datenschutzverletzung: Eine vergleichende Analyse der dauerhaften Identifizierung von Benutzern in sozialen Kontexten.* Federal Trade Commission (FTC) PrivacyCon 2020. Paper online über diesen Link verfügbar: <https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors>  Srinivasan, D. (2020). *Warum Google die Werbemärkte dominiert Die Wettbewerbspolitik könnte sich auf die Grundsätze der Finanzmarktregulierung stützen.* 24 STAN. TECHNIK. GESETZ REV. Von hier aus zugänglich: <https://law.stanford.edu/publications/why-google-dominates-advertising-markets/>  Warburton, N. (2020) Umschlaginnenseite des Buches von Véliz, C. (2020). *Datenschutz ist Macht: Warum und wie Sie die Kontrolle über Ihre Daten zurückerlangen sollten.* Penguin. |

**SCHRITT 4**

|  |  |
| --- | --- |
| **Schnitt 4 Titel** | **Ihre Rechte auf Privatsphäre** |
| **Schritt Lernergebnis** | 1. Beschreiben und diskutieren Sie die verschiedenen Aspekte der Privatsphäre. 2. Identifizieren und bewerten Sie die Art und Weise, wie personenbezogene Daten beim Surfen im Internet und der Nutzung von Apps auf Smart-Geräten erfasst werden. 3. Verstehen Sie die Rechte auf Privatsphäre, die sich aus Chartas zum Schutz unserer Daten ergeben. |
| **Thema** | Rechte auf Privatsphäre: UN-Menschenrechtscharta; EU-Charta der Menschenrechte; DSGVO |
| **Große Frage** | *Welche Rechte habe ich auf Privatsphäre?*  Fragen Sie Ihre Familie und Freunde, was sie über ihre Rechte auf Privatsphäre denken. Sie können Ihre Ansichten im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen:<https://csicop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Chartas und Vorschriften, die die Menschenrechte in Bezug auf die Privatsphäre einschließen. |
| **Lerninhalte** | **Menschenrecht auf Privatsphäre**  Um zusammenzufassen, was wir bisher gelernt haben:  • In Schritt 1 wurden wir in das Konzept der „Datenschutz“ eingeführt.  • In Schritt 2 haben wir erfahren, dass sich „personenbezogene Daten“ auf eine lebende Person beziehen  • In Schritt 3 haben wir einige Möglichkeiten kennengelernt, wie unsere Daten online erfasst werden können (z. B. durch Cookies).  In diesem Schritt werden wir „Menschenrechte“ untersuchen.  Pat Walshe von Privacy Matters erinnert uns daran, dass die Menschenrechte seit langem wichtig sind. Bereits [1689](https://www.webarchive.org.uk/wayback/archive/20131031165954/http:/www.bl.uk/onlinegallery/takingliberties/staritemshumanrights.html), beispielsweise in Großbritannien, galten die Menschenrechte als wesentlich für das Menschsein, für unsere Würde und den Schutz grundlegender Rechte und Freiheiten (British Library, 2013). Rechte und Freiheiten, die heute verschiedene Dimensionen unseres Lebens prägen – offline und online. Vom Recht auf freie Meinungsäußerung, über das Recht auf freien Umgang mit anderen und auf Versammlungsfreiheit, über die Religionsfreiheit, über das Recht auf Bildung, das Recht auf ein faires Verfahren, das Recht auf Eheschließung und auf zum Beispiel **das Recht auf Privatsphäre**. Menschenrechte sind wichtig. Jeden Tag. Offline und online. Sie ermöglichen uns, als Menschen zu gedeihen.  Menschenrechte in neuerer Zeit gewannen **1948** weltweite Bedeutung. Als Reaktion auf die Gräueltaten des Zweiten Weltkriegs verabschiedete die Generalversammlung der Vereinten Nationen die [Allgemeine Erklärung der Menschenrechte](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.un.org%2Fen%2Fabout-us%2Funiversal-declaration-of-human-rights&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344161263%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=uA%2B1stRDQLrowoxPVHRcaPjHo%2B0BT4CK0n60J364GWA%3D&reserved=0) (**UDHR**) zum Schutz der grundlegenden Menschenrechte, die allen Menschen zustehen sollten. Dies umfasst den Schutz vor willkürlichen Eingriffen in die **Privatsphäre, Familie, Wohnung oder Korrespondenz** einer Person gemäß Artikel 12 der AEMR.  1949 bildeten mehrere europäische Länder den [Europarat](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fyerevan%2Fthe-coe%2Fabout-coe%2Foverview&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344161263%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=JYIiQpLG0k8JcNGCurBcULLRd2iAd9iwASOg9yPWVOg%3D&reserved=0) (**CoE**), der derzeit 47 europäische Mitgliedstaaten vereint. **1950** verabschiedete der Europarat die [Europäische Menschenrechtskonvention](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.echr.coe.int%2FPages%2Fhome.aspx%3Fp%3Dbasictexts%26c%3D&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344171219%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=iickwfKhNhJyIxTdU3hZDPYgAeUvGbj0RG1KkT7fPBE%3D&reserved=0) (EMRK), um uns auch in Zukunft vor Gräueltaten wie denen des ZweitenWeltkriegs zu schützen. Die EMRK enthält die wichtigsten Rechte der AEMR und trat **1953** in Kraft. Die EMRK ist das erste **internationale rechtsverbindliche** Instrument zum Schutz der Menschenrechte. Bemerkenswert ist, dass alle Mitgliedstaaten der Europäischen Union (EU) der EMRK **beigetreten sind**.  Artikel 8 der EMRK sieht vor, dass jeder das Recht auf Achtung seines **Privat-** und **Familienlebens**, seiner **Wohnung** und seines **Briefverkehrs** hat. Es ist leicht zu erkennen, wie ein solches Recht intime Aspekte des Lebens einer Person schützen soll. Aspekte, die online leicht zu beobachten sind.  Während Artikel 8 der EMRK das Recht auf Privatsphäre schützt, umfasst er auch das Recht auf Datenschutz, da sich die Verwendung personenbezogener Daten über Personen nicht nur auf ihre Privatsphäre auswirkt, sondern auch auf andere Rechte und Freiheiten, auf die in diesem Kurs eingegangen wird. Um zum Schutz des Einzelnen und seiner Rechte und Freiheiten und insbesondere des Rechts auf Privatsphäre beizutragen, verabschiedete der Europarat 1981 eine Reihe von Grundsätzen und Regeln für die Verarbeitung personenbezogener Daten über Einzelpersonen. Die Grundsätze und Regeln sind als Konvention 108 bekannt. Die Konvention wurde vor kurzem modernisiert, um Veränderungen in der Technologie und der Datennutzung Rechnung zu tragen, die sich nachteilig auf die Rechte der Menschen auswirken können. Es ist jetzt bekannt als [Konvention 108+.](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fdata-protection%2Fconvention108%2Fmodernised&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4%2FyHZ6SiuxCw1AEWj0hVH0gYqGJA%2FbRQxow2%2F1Fazw0%3D&reserved=0)  Im Jahr **2000** hat die EU die [EU-Grundrechtecharta](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Ffra.europa.eu%2Fen%2Feu-charter&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=EWVDDZrcKGqL9KAMEwfgIVTWdQXjtz5dIRfobjVTtkk%3D&reserved=0) erstellt. Die Charta wurde 2009 für die Mitgliedsstaaten der EU rechtsverbindlich. Wie die EMRK sieht auch die Charta der Grundrechte der EU (**EU CFR**) vor, dass jeder das Recht auf Achtung seines **Privat-** und **Familienlebens**, seiner **Wohnung** und seiner **Kommunikation** hat (Artikel 7). Darüber hinaus sieht der **EU-CFR** auch vor, dass jeder das Recht auf den Schutz seiner personenbezogenen Daten hat (Artikel 8).  Artikel 7 und 8 des EU-GGR sehen jeweils ein Recht auf Privatsphäre und Datenschutz als zwei unterschiedliche Rechte vor. Diese Rechte werden durch ein **ePrivacy-Instrument**, bekannt als die EU-[ePrivacy-Richtlinie](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DOJ%3AL%3A2009%3A337%3A0011%3A0036%3Aen%3APDF&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4Vp99U43lyhjPuhTxYvnTnt81EYIefMk6pnaMHYdfEE%3D&reserved=0) (das für Dinge wie Cookies und andere Online-Tracking-Techniken gilt) und durch ein Datenschutzinstrument, die EU-[Datenschutz-Grundverordnung](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN) (**DSGVO**), verwirklicht. Die [Datenschutzvorschriften](https://eur01.safelinks.protection.outlohttps/ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_de) der EU und des Europarats wurden in das Recht der Mitgliedstaaten umgesetzt und verschärft, um den technologischen Veränderungen und der Datennutzung Rechnung zu tragen.  Wenn Menschen heute ihre Mobiltelefone oder Laptops usw. verwenden, können Daten über Menschen in Echtzeit gesammelt und beispielsweise zwischen Hunderten von Drittanbietern ausgetauscht werden, oft auf eine Weise, ohne dass die Leute sich wirklich bewusst sind oder eine sinnvolle Wahl treffen. Daten, die Aspekte des Privatlebens einer Person offenlegen können, wie beispielsweise ihr Standort, ihre Einkaufsgewohnheiten, die von ihr besuchten Websites, ihre Kontakte und ihre sozialen Verbindungen.  The UK Information Commissioner’s Office (ICO):  *„Die Datenschutz-Grundverordnung (DSGVO) von 2018 gibt Einzelpersonen das Recht, über die Erhebung und Verwendung ihrer personenbezogenen Daten informiert zu werden.* ***Dies ist eine wichtige Transparenzanforderung****“*  – auf der Website des ICO hier erklärt: <https://bit.ly/2QxmZH1>  Pat Walshe von Privacy Matters erklärt:  *„Ein Recht auf Privatsphäre und Datenschutz sind wichtiger denn je, da unsere digitalen Daten zutiefst persönliche und intime Aspekte von uns selbst und denen, mit denen wir verbunden sind, offenbaren“.*  Worauf Sie sich im nächsten Schritt freuen können  Im letzten Schritt dieses Kurses, Schritt 5, lernen wir *Online-Tools* kennen, mit denen wir *unsere Privatsphäre besser* *schützen und unsere Daten schützen können.*  Überprüfen Sie Ihr Lernen  Bitte überprüfen Sie, was Sie in Schritt 4 gelernt haben, mit einem Mini-Quiz im Abschnitt Aktivitäten. |
| **Überprüfen Sie Ihr Lernen** | **1948 Allgemeine Erklärung der Menschenrechte (UDHR): Artikel 12:**  *„Niemand darf willkürlichen Eingriffen in seine Privatsphäre … [oder] Korrespondenz“ ausgesetzt werden“.*  **2000 EU-Charta der Grundrechte (EHCR): Artikel 1:**  *„Die Würde des Menschen ist unantastbar. Sie muss respektiert und geschützt werden“.*  **Die Datenschutz-Grundverordnung (DSGVO) von 2018 „stellt hohe Anforderungen an die Einwilligung“:**  Diese Einwilligung ***nach Aufklärung*** beinhaltet:   * „*Einzelpersonen echte Wahlmöglichkeiten und Kontrolle bieten“* * *„echte Zustimmung sollte Einzelpersonen Verantwortung übertragen, Vertrauen und Engagement aufbauen“.* |
| **Aktivitäten** | Mini-Quiz zu den verschiedenen Chartas und Vorschriften.  Sind die folgenden Aussagen wahr oder falsch?   * Die UNHR ist eine neue Verordnung zur Erteilung der Einwilligung nach Aufklärung. * Die E-Datenschutzrichtlinie betrifft Cookies * Die DSGVO befasst sich nicht mit Transparenz.   Besprechen Sie Ihre Antworten mit Familie, Freunden, Nachbarn oder Kollegen.  Zur Erinnerung: Sie können Ihre Ansichten zu Ihrem Lernen im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie ein Login erstellen, hier: <https://csi-cop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Diskussion mit anderen Citizen Scientists über die Erklärung von Sun Microsystems, CEO und Mitbegründer, Scott McNealy aus dem Jahr 1999:  ***„Du hast sowieso null Privatsphäre …. Komm darüber hinweg!"***  Zitiert in Wired: <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> |
| **Lerninhalte** | Online-Privatsphäre ist kein Luxus |

|  |  |
| --- | --- |
| **Weiterführende Literatur für Schritt 4** | Links zum Weiterlesen, die in Schritt 4 erwähnt wurden, finden Sie, indem Sie den unterstrichenen Text unten auswählen:  **Literatur-Empfehlungen**  Britische Bibliothek (2013). *Take Liberties: Der Kampf um die Freiheiten und Rechte Großbritanniens*. Freiheiten nehmen – Star Items Index – Menschenrechte. Von hier aus erreichbar: <https://bit.ly/2QU4bSa>  ICO (kein Datum). *Leitfaden zur Datenschutz-Grundverordnung (DSGVO): Recht auf Auskunft. UK Information Commissioner's Office (ICO).* Von hier aus erreichbar: <https://bit.ly/3erd79K>  **Weiterlesen**  EHCR (kein Datum). *Europäische Menschenrechtskonvention.* Von hier aus erreichbar: <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=>  ePrivacy-Richtlinie (2002). *32002L0058 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie über den Datenschutz und die elektronische Kommunikation).*  Von hier aus zugänglich: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32002L0058&from=DE>  DSGVO (2016). *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Allgemeiner Datenschutz Verordnung).*  Von hier aus erreichbar: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=DE>  UNO (ohne Datum). *Erklärung der Menschenrechte der Vereinten Nationen.* Von hier aus erreichbar: <https://www.un.org/en/about-us/universal-declaration-of-human-rights> |

**SCHRITT 5**

|  |  |
| --- | --- |
| **Schnitt 5 Titel** | **So schützen Sie Ihre Daten online** |
| **Schritt Lernergebnis** | 1. Beschreiben und diskutieren Sie die verschiedenen Aspekte der Privatsphäre. 2. Identifizieren und bewerten Sie die Art und Weise, wie personenbezogene Daten beim Surfen im Internet und der Nutzung von Apps auf Smart-Geräten erfasst werden. 3. Verstehen Sie die Rechte auf Privatsphäre, die sich aus Chartas zum Schutz unserer Daten ergeben. |
| **Thema** | Tools zum Schutz Ihrer Daten im Internet. |
| **Große Frage** | *Wie ändere ich die App- und Webbrowser-Einstellungen, um das Online-Tracking zu beenden?*  Informieren Sie Ihre Familie und Freunde über die Tools, die ihnen helfen, ihre Daten online zu schützen. Sie können Ihre Ansichten im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie hier ein Login erstellen:<https://csicop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | **Apps**: Überprüfen Sie die Berechtigung in den "Einstellungen" für vorhandene Apps auf Ihren mobilen Geräten. Überprüfen Sie vor dem Herunterladen von Apps, welche Berechtigungen die App anfordert – sind diese erforderlich, damit die App funktioniert? Beispielsweise benötigt eine Transport-App Zugriff auf Ihren Standort, damit die App genaue Informationen bereitstellen kann.  **Websites:** Verwenden Sie einen Browser, der auf Datenschutz ausgelegt ist, oder aktualisieren Sie die Einstellung für kein Tracking und begrenzen Sie Werbe- und Marketing-Cookies von Drittanbietern. |
| **Lerninhalte** | Online-Tools, mit denen Sie Ihre Daten und Ihre Privatsphäre schützen können  Um zusammenzufassen, was wir bisher gelernt haben:   * In Schritt 1 wurden wir in das Konzept der „Datenschutz“ eingeführt. * In Schritt 2 haben wir erfahren, dass sich „personenbezogene Daten“ auf eine lebende Person beziehen * In Schritt 3 haben wir einige Möglichkeiten kennengelernt, wie unsere Daten online erfasst werden können (z. B. durch Cookies). * In Schritt 4 haben wir die verschiedenen Chartas und Vorschriften kennengelernt, die Ihnen das Recht auf Privatsphäre einräumen   In diesem Schritt werden wir herausfinden, welche Tools online verfügbar sind, um unsere Daten und unsere Privatsphäre zu schützen.  Wenn Sie an Ihre Internetnutzung denken, haben Sie das Gefühl, dass Sie mehr und mehr Zeit Ihres Lebens online verbringen als je zuvor?  Pat Walshe (Privacy Matters) stellt fest, dass wir online gehen, um: einzukaufen, Videoanrufe zu tätigen, uns Nachrichten zu senden, Erfahrungen, Gedanken und Gefühle über soziale Medien auszutauschen. Wir buchen auch Gesundheitstermine, recherchieren beispielsweise auch zu Gesundheitsthemen. Wir gehen auch online, um Wegbeschreibungen zu finden und zu befolgen – für die Anreise mit öffentlichen Verkehrsmitteln, Auto, Fahrrad oder zu Fuß. Wir hören auch online Musik oder Audio und schauen uns Filme oder Fernsehen im Internet an.  Ein Großteil unseres Lebens ist digital geworden. Aber die Digitalisierung schafft und hinterlässt digitale Fußabdrücke, digitale Daten, die gesammelt und verwendet werden können, um uns zu profilieren, über uns zu lernen und uns auf eine Weise zu beeinflussen, deren wir uns vielleicht nicht bewusst sind. Jede Webseite, die Sie besuchen; jedes Klicken und Tippen, das Sie machen; jeder Anruf oder jede Nachricht, die Sie tätigen oder empfangen; jeder Social-Media-Beitrag, den Sie machen; die Orte, die Sie besuchen oder „markieren“; jedes ‚Gefällt mir‘, das Sie machen; Die Songs, die Sie anhören, oder die Filme, die Sie sich ansehen (und Details dazu, wann Sie dies getan haben, ob Sie einen Titel oder Film angehalten, vorgespult oder übersprungen haben) erzeugen Daten. Dies sind Daten, die Aspekte Ihres Verhaltens, Aspekte von IHNEN und oft intime Aspekte von IHNEN offenbaren. Zum Beispiel Fruchtbarkeits-Apps, die Sie genau kennen. Siehe diesen Artikel des Wired-Magazins von 2018, „Bevor Sie Empfängnisverhütungs-Apps verwenden, denken Sie an Ihre Privatsphäre“: <https://bit.ly/3ajCyZz>.  Darüber hinaus berichtete eine Wohltätigkeitsorganisation für Datenschutz in einem Guardian-Artikel aus dem Jahr 2020, dass „Menstruations-Apps übermäßig viele Informationen speichern“. Hier könnt ihr es nachlesen: <https://bit.ly/3aj7IQH>.  Dann gibt es Apps, die zum Beispiel intime Aspekte der Sexualität, Religion oder ihres Standorts einer Person teilen (und "Standortdaten" können sehr viel vermuten lassen – ob es sich bei einem Standort um einen Ort einer bestimmten Art von Anbetung oder eine Gesundheitsklinik einer bestimmten Art handelt Natur). Sehen Sie sich diesen Verbraucherbericht 2020 über solche Apps hier an: <https://bit.ly/3ggUw2x>.  Aber Daten offenbaren nicht nur Aspekte von DIR, sondern auch Aspekte von ANDEREN. Von denen, mit denen Sie kommunizieren und mit denen Sie Informationen austauschen, von Ihren Beziehungen und Kommunikationsmustern. Beispielsweise kann eine App Sie auffordern, die auf Ihrem Computer oder Smartphone gespeicherten „Kontakte“ hochzuladen oder ihnen Zugriff zu gewähren. Aber was steckt in einem Kontakt? Ein Kontakt kann den Namen, das Bild, die Handynummer, die E-Mail-Adresse, die Postanschrift, den Namen der sozialen Medien und das Jubiläumsdatum einer Person enthalten. Digital online zu sein, erfordert möglicherweise, dass wir nicht nur an unsere eigene Privatsphäre denken, sondern auch an die Privatsphäre anderer.  Wie in Schritt 4 erläutert, ist das Recht auf Online-Datenschutz in der EU und im Vereinigten Königreich durch spezifische **ePrivacy-Gesetze** und die **Datenschutz-Grundverordnung (DSGVO)** geschützt. Aber Gesetze und ihre Durchsetzung können nur eine begrenzte Menge bewirken. Es gibt Dinge, die Sie tun können, um Ihre Privatsphäre online zu schützen.  In Schritt 3 haben wir erfahren, wie Personen **über das Web** verfolgt werden. Dies umfasst Werbetechnologien (Ad-Tech) wie Cookies, serverseitiges Tracking. Aber was können Sie tun, um es zu kontrollieren und Ihre Privatsphäre online zu schützen? [[Privatsphäre-Selbstverwaltung](https://policyreview.info/pdf/policyreview-2020-4-1537.pdf) ist schwer]. Sie können mehr darüber erfahren, wie Personen **über mobile Apps** (Software Development Kits – SDKs) [verfolgt werden](https://privacyinternational.org/case-study/4404/mobile-app-monetisation-covert-trackers-your-pocket), indem Sie einen Artikel von Binns et al. (2018): „Third Party Tracking in the Mobile Ecosystem“, abrufbar hier: <https://arxiv.org/pdf/1804.03603.pdf>  **Tools, um Tracking zu entdecken und zu kontrollieren.**  **Transparenztools - Web:**  Es gibt eine Reihe von Tools, die Ihnen helfen, das Tracking auf den von Ihnen besuchten Websites zu verstehen. Ein Großteil des Trackings wird durchgeführt, um Sie mit Werbung anzusprechen oder Ihre Erfahrung zu „personalisieren“. Dies beinhaltet oft den Austausch von Daten mit Werbeunternehmen von Drittanbietern, manchmal Hunderten von Unternehmen.  **Einige der Web-Transparenz-Tools umfassen:**  **Webbkoll** ist ein Tool, das simuliert, was passiert, wenn ein Benutzer eine Webseite mit einem typischen Browser besucht. Es wird angezeigt, welche Cookies von Erstanbietern und Drittanbietern auf der besuchten Seite vorhanden sein können und auch welche Nachverfolgung stattfindet, die nicht auf Cookies basiert, wie z. B. Anfragen von Servern: <https://webbkoll.dataskydd.net/en>  **Blacklight** scannt eine Website und zeigt wichtige Tracking-Technologien auf der Website an: <https://themarkup.org/blacklight>  **Pagexray** ist ein Analysetool, das alle auf einer Webseite geladenen Anzeigen und Tracker anzeigt und die Ergebnisse in Form eines Baumdiagramms darstellt. Ergebnisse können als HTTP-Archiv (.har.json) oder detaillierte Ergebnisse (.json) heruntergeladen werden**:** <https://requestmap.webperf.tools>  **Cover Your Tracks** ist ein Tool zum Testen, wie gut Ihr Browser vor Tracking und Fingerprinting schützt https://coveryourtracks.eff.org  **Transparenztools – Mobile Apps:**  Mobile Apps zu untersuchen ist nicht einfach. Wenn Sie Apps auf Ihrem Telefon verwenden, erklärt [O’Flaherty](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/), ein Cybersicherheitsjournalist, dass die Apps „Sie möglicherweise über andere Apps und Websites hinweg verfolgen, um Sie mit Werbung anzusprechen. Dies geschieht derzeit über eine sogenannte Kennung für Werbetreibende (**IDFA**), die verfolgt, ohne Ihre persönlichen Daten preiszugeben.  Es gibt einige Tools, die helfen, die Existenz von „Trackern“ zu beleuchten, die in Android-Apps eingebettet sind.  Ein wichtiges Tool für Android ist **Exodus Privacy**: <https://exodus-privacy.eu.org/en/>  Android-Studio: <https://developer.android.com/studio>  Pat Walshe (Privacy Matters) weist darauf hin, dass es derzeit kein gleichwertiges Tool für Apples iOS-Apps gibt. Apple hat jedoch neue Transparenzregeln für seinen Store und seine Entwickler eingeführt, die von ihnen verlangen, vordefinierte Datenschutzkennzeichnungen zu verwenden, um offenzulegen, welche Daten sie verwenden und warum. Apples neues [iOS 14.5](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.apple.com%2Fnewsroom%2F2021%2F04%2Fios-14-5-offers-unlock-iphone-with-apple-watch-diverse-siri-voices-and-more%2F&data=04%7C01%7Cab7778%40coventry.ac.uk%7C0961dc6c3373461cef5308d9096cf9ba%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637551185936139952%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=yZzrdJ2Qdo3qBjKRGUWHNO5wjKePxo4%2BYYrWf3M4sHM%3D&reserved=0) erfordert auch, dass Entwickler  *„die Erlaubnis des Benutzers einholen, bevor sie ihre Daten über Apps oder Websites, die anderen Unternehmen gehören, zu Werbezwecken verfolgen oder ihre Daten an Datenbroker weitergeben“.*  Laut Apple ermöglicht die neue Datenschutzfunktion Besitzern von Apple-Telefonen mit diesem Betriebssystem, „auf die Schaltfläche „Datenschutzbericht“ zu tippen, um besser zu verstehen, wie Websites mit Ihrer Privatsphäre umgehen. ([Apple, 2021](https://www.apple.com/uk/ios/ios-14/)). Laut Apple wird die App-Tracking-Transparenzfunktion (ATT) "erfordern, dass alle Apps eine ausdrückliche Erlaubnis zum Tracking anfordern" und  *"In den Einstellungen können Benutzer sehen, welche Apps die Erlaubnis zum Tracking angefordert haben, und Änderungen vornehmen, während sie für richtig halten.“* ([O’Flaherty, 2021](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/)).  Unter Mac OS („Big Sur“) bietet Apple ein Datenschutz-Berichtstool an, das als Symbol im Safari-Browser angezeigt wird. Auf diese Weise können Benutzer sehen, welche Tracker sich auf einer Webseite befinden und blockiert werden. Apple‘s Safari-Browser „bietet Ihnen mehr Möglichkeiten, Ihre Privatsphäre zu schützen“ ([Apple, 2021](https://www.apple.com/uk/ios/ios-14/)). Apple‘s Privacy Drive ist laut [O’Flaherty 2021](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/) ein „Game Changer“.  Und mit dem „Drittanbieter-Cookie-Sterben“ ([Cyphers, 2021](https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea)) könnten Citizen Scientists die treibende Kraft sein, die jeden Ersatz verhindert, uns online zu verfolgen, wie etwa Googles „neue Suite von Technologien zur zielgerichteten Werbung im Web“, die uns bewegen näher am Privatsphäre-Browsing.  **Zusammenfassung:** Was können Sie tun, um Ihre Privatsphäre zu schützen?  Browser  Werbeblocker  Datenschutzeinstellungen verwenden – Betriebssysteme, Browser, Apps. |
| **Überprüfen Sie Ihr Lernen** | Bitte überprüfen Sie, was Sie in Schritt 5 gelernt haben, indem Sie verstehen, dass es Möglichkeiten gibt, Ihre Daten und Ihre Privatsphäre zu schützen, wenn Sie online sind. |
| **Aktivitäten** | Erfahrungsbasiertes Lernen: Lernen Sie durch das Erkunden der von Ihnen besuchten Websites und der von Ihnen verwendeten Apps, welche digitalen Tracker, falls vorhanden, auf den Websites und in den Apps vorhanden sind.  **Aktivität 1:**  Verwenden Sie eines der Tools, die Sie in diesem Schritt kennengelernt haben, z. B. webbkoll, um eine Website zu erkunden, die Sie häufig besuchen. Überprüfen Sie die Website auf ihre a) Datenschutzrichtlinie und b) ihren Cookie-Hinweis.  **Fragen**  -Wie leicht war die Datenschutzerklärung zu verstehen?  -Hat der Cookie-Hinweis über irgendwelche und die Anzahl der Cookies informiert?  -Welche eingebetteten Drittanbieter-Cookies wurden Ihnen im Cookie-Hinweis bekannt gegeben?  **Aktivität 2:**  Überprüfen Sie die Berechtigungen einer App auf Ihrem Mobilgerät. Gehen Sie zu „Einstellungen“ und wählen Sie eine beliebige App aus und überprüfen Sie deren Berechtigungen.  **Fragen**   * Welche Berechtigungen wurden der von Ihnen überprüften App erteilt? * Wussten Sie diese Berechtigungen für die App, als Sie sie heruntergeladen haben?   Zur Erinnerung: Sie können Ihre Meinung zu Ihrem Lernen im CSI-COP-Website-Forum hier posten: <https://csi-cop.eu/forum/> - Sie müssen sich auf der Website registrieren, bevor Sie im Forum posten, indem Sie ein Login erstellen, hier: <https://csi-cop.eu/citizenscientistlogin/> |
| **Kurze Zusammenfassung** | Aufstieg vom informellen Lernenden zum CSI-COP Citizen Scientist.  Besprechen Sie Ihre Meinung zu diesem Workshop mit Familie und Freunden:   * Was haben Sie Ihrer Meinung nach durch die fünf informellen Lernschritte des CSI-COP gewonnen? * Möchten Sie dem CSI-COP-Team beitreten und Citizen Scientist werden, um Online-Tracking zu untersuchen? * Haben Sie Interesse an Weiterbildungen zu Datenschutz, Datenschutz, Webentwicklung und verwandten Themen? |
| **Lerninhalte** | Ich schütze meine Daten mit Webtools. |

|  |  |
| --- | --- |
| **Weiterführende Literatur für Schritt 5** | Literatur-Empfehlungen  Cyphers, B. (2021). *Google’s FLoC (Federated Learning of Cohorts) ist eine schreckliche Idee.* **Electronic Frontier Foundation.**  Von hier aus erreichbar: <https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea>  O’Flaherty, K. (2021). *Apple’s atemberaubender iOS14 Privacy Move: ein Game-Changer für alle iPhone-Benutzer.* **Forbes.**  Von hier aus erreichbar: <https://bit.ly/3vpOq4v/> |

**Ihre Rückmeldung**

|  |  |
| --- | --- |
| Ihr Feedback zum informellen Schulungskurs von CSI-COP „Ihr Recht auf Online-Privatsphäre“ | Es würde dem CSI-COP-Team helfen zu wissen, wie nützlich Sie diesen Kurs fanden. Bitte wählen Sie einen aus der folgenden Liste aus:  5. Sehr nützlich  4. Nützlich  3. Keine Gedanken  2. Nicht nützlich  1. Definitiv nicht nützlich  Bitte zögern Sie nicht, weitere Kommentare oder Vorschläge zu diesem Kurs hinzuzufügen: |

**Bewerten Sie Ihr Lernen**

Um Ihr Lernen zu bewerten und ein CSI-COP-Zertifikat zu erhalten, beantworten Sie bitte die Fragen und senden Sie entweder Huma oder Jaimz an die untenstehenden E-Mails. Wenn Sie 8/10 erreichen, erhalten Sie ein informelles CSI-COP-Ausbildungszertifikat. Sie können die Fragen beliebig oft ausprobieren und Ihre Antworten an das CSI-COP-Team der Coventry University senden:

Huma: [ab7778@coventry.ac.uk](mailto:ab7778@coventry.ac.uk) oder

Jaimz: [ad5956@coventry.ac.uk](mailto:ad5956@coventry.ac.uk)

**Fragen**

1. Ist diese Aussage wahr oder falsch: Datenschutz ist seit Facebook ein Thema?
2. Ist diese Aussage richtig oder falsch: Mit dem Inkognito-Browser von Google Chrome können Sie absolut vertraulich suchen?
3. Ist diese Aussage richtig oder falsch: Wenn Sie öffentliches WLAN verwenden, können Sie Ihre Standortdaten teilen?
4. Ist diese Aussage richtig oder falsch: Sensible personenbezogene Daten beziehen sich auf Ihren Namen?
5. e. Ist diese Aussage richtig oder falsch: Fingerabdruck ist eine Form des Website-Trackings, die die Attribute Ihres Geräts oder Browsers verwendet, um ein Profil von Ihnen zu erstellen?
6. Welche Klassen als Verhaltensdaten – bitte wählen Sie unten alle zutreffenden aus:
7. Ihre Interaktionen auf einer Website
8. Ihre Webbrowser-Daten
9. Online-Kaufhistorie
10. Wenn Sie eine Online-Karte verwenden
11. Verwenden einer App, um beispielsweise Ihren Gesundheitszustand zu überwachen
12. Ist diese Aussage wahr oder falsch: Die Menschenrechte wurden als etwas Wesentliches für unsere Würde und den Schutz der Grundrechte und -freiheiten angesehen?
13. Ist diese Aussage wahr oder falsch: Zu Ihren Rechten gemäß der Allgemeinen Erklärung der Menschenrechte (UDHR) gehört der „*Schutz vor willkürlichen Eingriffen in die Privatsphäre, Familie, Wohnung oder Korrespondenz einer Person“*?
14. Ist diese Aussage richtig oder falsch: Laut Europäischer Menschenrechtskonvention (EMRK): Wir haben in der Moderne keinen Anspruch auf Privat- und Familienleben in unserer Wohnung und unserem Briefverkehr?
15. Bitte wählen Sie nach der Datenschutzgrundverordnung (DSGVO) alles Zutreffende aus:
16. Recht auf Information
17. Recht auf Transparenz
18. Recht auf Datenschutz
19. Recht, nicht von der Kameraausrüstung anderer Personen gefilmt zu werden

**Citizen Scientist werden**

|  |  |
| --- | --- |
| **CSI-COP Citizen Scientist werden** | Möchten Sie nach Abschluss der fünf Schritte des informellen Schulungskurses von CSI-COP und Erhalt Ihres Zertifikats dem CSI-COP-Team beitreten und den Umfang des Online-Trackings untersuchen?  Sie können dem CSI-COP-Team beitreten und sich als Citizen Scientist im CSI-COP-Projekt engagieren.  Vollständige Informationen werden Ihnen auf Anfrage zur Verfügung gestellt, einschließlich:   * Teilnehmerinformationsblatt zum Zweck der Rolle des Citizen Scientists * Einwilligungserklärung gemäß Datenschutzgrundverordnung (DSGVO) * Informationen zu den ersten Schritten bei der Untersuchung von Websites und Apps auf Cookies.   Sie können jetzt mehr erfahren, indem Sie die '[About'](https://csi-cop.eu/about/)-Seite der CSI-COP-Website besuchen: <https://csi-cop.eu/about/>  Falls noch nicht geschehen, können Sie Ihr Interesse anmelden, indem Sie hier ein Konto auf der CSI-COP-Website erstellen: <https://csi-cop.eu/citizenscientistlogin/>  Das CSI-COP-Website-Forum, um mit anderen Citizen Scientists in diesem Projekt zu diskutieren, finden Sie hier: <https://csi-cop.eu/forum/>  Umseitig finden Sie unsere Umfrageinformationen und einige Fragen zu Ihrer Person. Dies soll CSI-COP helfen zu lernen, wer Citizen Scientists sind. Wir werden keine Daten erheben, die Sie als Person identifizieren. Wir schätzen Ihre Zeit. |

**CSI-COP-Umfrage 1**

|  |  |
| --- | --- |
| **Altersbereich: Bitte kreisen Sie einen aus dem Bereich ein** | 18-39; 40-65; 66+; Mache lieber keine Angabe |
| **Geschlecht: Bitte wählen Sie eines aus** | Weiblich; Männlich; Intersexuelle; Trans-Regenschirm; Andere;  Mache lieber keine Angabe |
| **Ort: Bitte wählen Sie einen aus** | Urban – Städte und Gemeinden – z.B. Patras, Coventry, London  Ländlich – Dörfer (unter 2000 Einwohner)  Mache lieber keine Angabe |
| **Sprachen:**  1. Was ist Ihre dominante oder Muttersprache?  2. Sprechen Sie mehr als eine Sprache fließend?  Sie können es vorziehen, es nicht zu sagen. | 1.  2.  Mache lieber keine Angabe |
| **Barrierefreiheit:**  Haben Sie Probleme mit der Zugänglichkeit? z.B. aufgrund einer Sehbehinderung Text-to-Speech-Software verwenden? | Ja  Nein  Mache lieber keine Angabe |
| **Arbeiten:** | Schülerniveau: bitte auswählen   * Bachelor * Postgraduierte * Doktorat   Nicht-Student: Bitte wählen Sie die Kategorie aus, die Ihren Beschäftigungsstatus am besten beschreibt:   * Angestellt, 36,5 oder mehr Stunden pro Woche arbeiten * Angestellt, Arbeitszeit 1-36 Stunden pro Woche * Nicht erwerbstätig, auf der Suche nach Arbeit * Nicht erwerbstätig, keine Arbeit suchen * Asylsuchender Flüchtling * Im Ruhestand * Probleme mit der Zugänglichkeit haben, nicht in der Lage zu arbeiten * Mache lieber keine Angabe |
| **Internet Zugang:** | Zugang zu einer eigenen Internetverbindung haben (Breitband/Mobil zu Hause oder am Arbeitsplatz)  Verwenden Sie den öffentlichen Zugang, wenn Sie das Internet nutzen  Mache lieber keine Angabe |
| **Internetnutzung:**  Wie oft benutzt du das Internet? Bitte auswählen: | Täglich  2-3-Mal die Woche  Wöchentlich  Weniger als einmal pro Woche  Noch nie  Mache lieber keine Angabe |
| **Zweck der Internetnutzung:** | Nutzen Sie das Internet   * als Teil der täglichen Arbeit * für die Freizeit, nicht für die Arbeit * für Arbeit und Freizeit   Verwenden Sie das Internet in eingeschränkter Weise, zum Beispiel mit einem Computer in einer öffentlichen Bibliothek.  Mache lieber keine Angabe |
| **Apps-Nutzung: Desktops und Laptops** | Verwenden Sie Apps regelmäßig, um beispielsweise den Zugriff auf Arbeitstools (z. B. Zoom, MS Teams) zu authentifizieren. Geben Sie in diesem Fall bitte die Namen einiger von Ihnen genutzter Apps und deren Zweck an:   * Arbeitstools (z. B. Microsoft Office, etc.) * Spiele spielen (z. B. STEAM). * Bildungs-Apps * Lebensstil (Sport, Fitness, Gesundheit) * Nachrichten * Unterhaltung (z. B. Streaming-Apps wie Netflix) * Andere * Mache lieber keine Angabe   Verwenden Sie selten Apps auf Desktops und Laptops  Verwenden Sie keine Apps auf Desktops und Laptops  Mache lieber keine Angabe |
| **Apps-Nutzung: Mobilgeräte** | Verwenden Sie regelmäßig Apps, z. B. Transport-Apps, um sich über die Fahrzeiten des nächsten Zuges, Busses usw. zu informieren. Wenn ja, nennen Sie bitte einige von Ihnen verwendete Apps und deren Zweck:   * Spiele spielen * Bildungs-Apps * Lebensstil (Sport, Fitness, Gesundheit): * Nachrichten * Unterhaltung (z. B. Streaming-Apps – Amazon Prime): * Andere * Mache lieber keine Angabe   Verwenden Sie selten Apps auf Mobiltelefonen oder Tablets  Keine Apps verwenden  Mache lieber keine Angabe |
| **Wie sind Sie auf das CSI-COP-Projekt aufmerksam geworden?** | Von der CSI-COP-Website  Von einer Universität  Von der Mitgliedschaft zu einem Verein (z.B. Women in Tech)  Von einer Citizen-Science-Plattform zum Beispiel   * SciStarter * Zoouniversum * EU-Bürger.Wissenschaft * Andere Citizen-Science-Plattform   Im Internet surfen  Bisherige ehrenamtliche Tätigkeiten  Sagen Sie bitte in den sozialen Medien, welche Plattform  Mundpropaganda  Andere |
| **Haben Sie den kostenlosen Online-Workshop für informelle Bildung von CSI-COP absolviert?** | Ja  Noch nicht, aber beabsichtigen  Nein, lieber auf zukünftige Präsenzworkshops warten, wenn diese in der Nähe meines Wohnortes stattfinden. |
| **Wenn Sie den Workshop abgeschlossen haben, beabsichtigen Sie, als ehrenamtlicher Citizen Scientist dem CSI-COP-Team beizutreten?** | Ja  Könnte sein  Ich brauche mehr Informationen  Nein |
| **Um Ihre ausgefüllten „Beurteilen Sie Ihr Lernen“-Fragen, Ihre Umfrage und für alle anderen Fragen zu senden, wenden Sie sich bitte an das CSI-COP-Team der Coventry University:** | Bitte senden Sie dieses ausgefüllte Dokument an die CSI-COP-Teammitglieder der Coventry University zurück:  Huma: [ab7778@coventry.ac.uk](mailto:ab7778@coventry.ac.uk) oder  Jaimz: [ad5956@coventry.ac.uk](mailto:ad5956@coventry.ac.uk) |
| Vielen Dank, dass Sie sich die Zeit genommen haben, den informellen Bildungskurs des CSI-COP und die Umfrage zu absolvieren  Dieses Dokument wird in Kürze in anderen Sprachen verfügbar sein.  Bitte besuchen Sie die CSI-COP-Website hier: [**https://csi-cop.eu/**](https://csi-cop.eu/) | |