

# Datenschutz bei PC's und Smartphones

**Betreuer:** Sascha Ludwig  
[ludwig@informatik.uni-leipzig.de](mailto:ludwig@informatik.uni-leipzig.de)  
Raum: P-818  
Telefon: 0341 97 32257

## Hintergrund und Zielstellung:

Das Thema „Datenschutz bei PC's und Smartphones“ beschäftigt sich hauptsächlich mit den Bereichen des Tracking und der Profilbildung sowie Gegenmaßnahmen gegen diese. Dabei liegt der Fokus zur Hälfte auf herkömmlichen PC's und Webbrowsern sowie zur anderen Hälfte bei Smartphones. Diese beiden Systeme unterscheiden sich in der Art der erhobenen Daten stark. Die TeilnehmerInnen sollen hierbei nicht nur Recherchearbeiten zum Thema leisten sondern sich auch Gedanken über eine eigene, prototypische (Selbst-)Datenschutz-App machen. Das Team bearbeitet folgende 6 Themenblöcke á 2 Wochen Bearbeitungszeit:

- Einarbeitung in das Thema Datenschutz, Tracking und Profilbildung
- Gegenmaßnahmen zu Tracking. Erhöhung der Privatsphäre
- Analyse einer Datenschutzerklärung über die Zeit
- Unterschiede PC's zu Smartphones bzgl. Datenschutz
- Anforderungen an eine Datenschutz-App
- Grafische Visualisierung der Datenschutz-App

## Detaillierter Aufgabenplan:

Angestrebt werden 6 Aufgabenblöcke á 2 Arbeitswochen. Die ersten drei Termine beschäftigen sich mit Datenschutz auf Webseiten und am PC. Die letzten drei Termine verlegen den Fokus auf mobile Endgeräte und deren Apps. Eine genaue Auflistung der Aufgaben und der erwartete Resultate finden sich in den untenstehenden Tabellen.

Termin	Thema	Aufgabenbeschreibung bzw. Fragestellungen	Erwartete Resultate
1	Einarbeitung in das Thema Datenschutz, Tracking und Profilbildung	<ul style="list-style-type: none"> <li>• Was ist Datenschutz und warum ist dieser wichtig?</li> <li>• Welche Trackingmethoden gibt es bei Webbrowsern?</li> <li>• Was ist Profilbildung und warum wird dieses betrieben?</li> <li>• Optional: Fallbeispiel zu Datenschutz in der Presse</li> </ul>	<ul style="list-style-type: none"> <li>• Definition(en) von Datenschutz (deutsches Recht) wurden recherchiert</li> <li>• Mindestens 3 Trackingmethoden (Web-Beacons+IP-Adressen, Javascript-Fingerprinting, Cookies, LogIn, Social Media Buttons, ...) wurden recherchiert</li> <li>• Gründe für Profilbildung wurden recherchiert</li> <li>• Ergebnisse wurden in einem mindestens 6-seitigen Bericht aufbereitet und zusammengefasst</li> </ul>
2	Gegenmaßnahmen zu Tracking, Erhöhung der Privatsphäre	<ul style="list-style-type: none"> <li>• Welche Gegenmaßnahmen können zu Tracking bei Webbrowsern getroffen werden?</li> <li>• Welche Vor- und Nachteile haben diese Methoden?</li> <li>• Interessant: <a href="https://panoptlick.eff.org/">https://panoptlick.eff.org/</a>, <a href="https://www.browserleaks.com/">https://www.browserleaks.com/</a>, <a href="http://ip-check.info/">http://ip-check.info/</a></li> <li>• Wie können diese Maßnahmen an Außenstehende gut vermittelt werden?</li> <li>• Optional: Gesetze und Gerichtsurteile zur Datenweitergabe</li> </ul>	<ul style="list-style-type: none"> <li>• Mindestens 5 Gegenmaßnahmen wurden recherchiert (Dienste konfigurieren, Browser-PlugIns: User Agent – Cookies – Do Not Track – Werbeblocker, Tor, Verschlüsselung, Anonymisierung, Ausstieg aus Diensten, ...)</li> <li>• Vor- und Nachteile von Gegenmaßnahmen wurden erörtert</li> <li>• Ein didaktisches Konzept wurde skizziert</li> <li>• Erkenntnisse aus Termin 1 und 2 wurden grafisch anspruchsvoll aufbereitet und zusammengefasst sodass sie gut von Außenstehenden verstanden und konkret umgesetzt werden können.</li> </ul>
3	Analyse einer Datenschutzerklärung über die Zeit.	<ul style="list-style-type: none"> <li>• Wie verändern sich Datenschutzbestimmungen über die Zeit? <ul style="list-style-type: none"> <li>◦ Wie können Vorgängerversionen gefunden werden?</li> <li>◦ Hierfür sollen von mindestens 5 Webseiten oder Apps die Datenschutzbestimmungen in der Zeit zurückverfolgt werden. Aus diesen 5 DSE soll eine interessante ausgewählt und näher betrachtet werden:</li> </ul> </li> <li>• Welche Unterschiede gibt es zwischen den Versionen?</li> <li>• Wie sind die Veränderungen zu bewerten (aus Nutzer- und Betreibersicht)?</li> <li>• Optional: Einschätzung der Datenschutzbeauftragten</li> </ul>	<ul style="list-style-type: none"> <li>• Mechanismus zum Erhalten von Vorgängerversionen von DSE wurde recherchiert (z.B: <a href="https://archive.org/web/">https://archive.org/web/</a> oder Archive einzelner Seiten)</li> <li>• ein DIFF-Tool wurde ausfindig gemacht und benutzt</li> <li>• Aus 5 Webseiten wurde eine passende und interessante DSE-Historie ausgewählt und genauer untersucht</li> <li>• Mechanismus, Diff-Tool und das Vorgehen wurden dokumentiert</li> <li>• Es wurde dokumentiert, wie zu den 5 Webseiten die DSE-Versionen gefunden wurden, wie viele Versionen es gibt und warum sich für die eine DSE entschieden wurde.</li> <li>• Unterschiede zwischen den Versionen wurde herausgearbeitet, grafisch oder tabellarisch aufbereitet und bewertet.</li> </ul>

Termin	Thema	Aufgabenbeschreibung bzw. Fragestellungen	Erwartete Resultate
4	Unterschiede PC's zu Smartphones bzgl. Datenschutz	<ul style="list-style-type: none"> <li>• Welche Unterschiede gibt es vom Webbrowser (PC) zu Smartphones?</li> <li>• Welche Daten können hier (zusätzlich / weniger) erhoben werden? <ul style="list-style-type: none"> <li>◦ Welche Eigenschaften haben diese Daten?</li> </ul> </li> <li>• Wie ist ein Tracking und Profilbildung hier möglich? <ul style="list-style-type: none"> <li>◦ Welche auf den ersten Blick ungewöhnlichen Methoden gibt es</li> </ul> </li> <li>• Optional: Gegenmaßnahmen</li> </ul>	<ul style="list-style-type: none"> <li>• Unterschiede wurden recherchiert</li> <li>• eine Liste an verfügbaren Daten und deren Eigenschaften (veränderbar, statisch, leicht zu ändern, leicht zu fälschen, ...) wurden erstellt</li> <li>• Trackingmethoden wurden herausgearbeitet (GPS-Tracking, WiFi-Kennungen-Tracking, Fingerprinting über Geräteinformationen, Google- bzw. Apple-Konto, ...)</li> </ul>
5	Anforderungen an eine Datenschutz-App	<p>Unter der Annahme perfekten Wissens über alle installierten Apps auf einem Smartphone (z.B. alle Datenflüsse, Funktionen, DSE-Texten usw.)</p> <ul style="list-style-type: none"> <li>• Wie kann eine mobile App zur Förderung des (Selbst)Datenschutzes aussehen?</li> <li>• Welche Funktionen sollte diese App haben?</li> <li>• Wie können Nutzer zu mehr (Selbst)Datenschutz motiviert werden?</li> </ul>	<ul style="list-style-type: none"> <li>• Aufbau, Ablauf und Funktionsweise einer prototypischen App wurden schriftlich und evtl. auch grafisch skizziert</li> <li>• ein didaktisches Konzept zur Motivation der Nutzer zu mehr (Selbst)Datenschutz wurde skizziert</li> </ul>
6	Grafische Visualisierung der Datenschutz-App	<ul style="list-style-type: none"> <li>• Grafischer Entwurf der App</li> <li>• Interessant: Wireframes: proto.io</li> </ul>	<ul style="list-style-type: none"> <li>• Teile der App wurden als grafische MockUps realisiert</li> </ul>

#### Text-Ressourcen:

- Heise
- Chaos Computer Club
- offizielle Seite der Datenschutzbeauftragten: <http://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html>

#### Software-Ressourcen:

- DIA, Libre Office Draw, GIMP, InkScape
- proto.io
- <https://www.diffchecker.com/>, KDiff3, ExamDiff, GIT
- Libre Office, Microsoft Office, LaTeX