

---

# Usability trifft DSGVO:

Wie gehe ich mit sensiblen  
Daten um?

AK Usable Security & Privacy  
Workshop Mensch und Computer  
Hamburg, 10.09.2019



**GERMAN UPA**

Berufsverband der Deutschen Usability  
und User Experience Professionals

---

# Warum Usable Security & Privacy?





---

# Wie nehmen UUX-Professionals die Situation wahr?

## Größte Herausforderungen/Probleme in diesem Bereich?<sup>1</sup>

Sicherheitsfeatures werden nicht nutzerzentriert entwickelt. 49 %

Mir fehlt eigenes Fachwissen zu IT-Security- bzw. Privacy-Themen. 47 %

## Was würde Dir bei Deiner Arbeit weiterhelfen?<sup>2</sup>

Methodenwissen zum Thema Usable Security & Privacy 57 %

spezialisierte Werkzeuge für Usable Security & Privacy,  
z. B. Richtlinien, Patterns, Checklisten 52 %

Quelle: German UPA Mitgliederbefragung 2018

(n = 184<sup>1</sup> bzw. 170<sup>2</sup>)



---

# Arbeitskreis Usable Security & Privacy



Arbeitskreistreffen an der TH Köln, 26. April 2019  
(Bildrechte: Michael Schuff, TH Köln)



# Woran wir arbeiten

- Fachschrift
- UPA-Website: Blogbeiträge mit Empfehlungen zu DSGVO, Passwortsicherheit, Passwortmanager ...
- Webinar
- Mitgliederbefragung
- Literatursammlung auf GitHub
- Veranstaltungen, z. B. MCI, Privacy Week Berlin, WUD
- Vernetzung, z. B. UXPA, GI
- regelmäßige Telefonkonferenzen, AK-Treffen

The screenshot shows a browser window displaying the website for the German UPA Working Group Usable Security & Privacy. The page features the organization's logo and name, followed by the title 'Usable Security and Privacy Reading List'. Below the title, there is a paragraph explaining that the page collects literature worth reading from the field of Usable Security and Privacy, managed by the German UPA and open to contributions. At the bottom of the visible text, there are filter options for authors, keywords, and category, and the beginning of a list entry titled 'Usability Meanings and Interpretations in ISO Standards'.



---

## Wer wir sind

- Anne Hofmeister, Technische Hochschule Köln
- Arkadiusz Frydyada de Piotrowski, CONDEPIO - Consulting Frydyada de Piotrowski
- Denis Feth, Fraunhofer-Institut für Experimentelles Software Engineering IESE
- Gina Maria Schmidbauer-Wolf, TU Darmstadt
- Hannes Johne, BIM Berliner Immobilienmanagement GmbH
- Hartmut Schmitt, HK Business Solutions GmbH
- Jessica Miriam Zinn, User Experience Consultant
- Leo Heuser, Hochschule Hamm-Lippstadt
- Luigi Lo Iacono, Technische Hochschule Köln
- Mandy Balthasar, Universität der Bundeswehr München
- Markus Dölle, User Experience Consultant
- Nina Gerber, KIT - Karlsruher Institut für Technologie
- Timo Jakobi, Universität Siegen

Arbeitskreis Usable Security & Privacy



# Woran wir sonst arbeiten

TrUSD – Transparente und selbstbestimmte  
Ausgestaltung der Datennutzung im Unternehmen

<https://www.trusd-projekt.de/>

Datenanalyse im Unternehmen vs. Recht der  
Beschäftigten auf Privatheit

Privacy Dashboards

- mehr Transparenz für Arbeitnehmer
- Möglichkeiten der Selbstbestimmung

Rahmenwerk, Demonstratoren, Evaluation ...

The screenshot shows the website <https://www.trusd-projekt.de/>. The page features a navigation menu with links for Start, Projekt, Partner, Glossar, and Kontakt. The main content area displays a large image of a laptop with various data visualization icons (pie charts, bar graphs, dollar signs, padlocks) on its screen. Below the image, there is a search bar and a list of articles. The first article is titled "5. Usable Security und Privacy Workshop" and includes details about the event at the University of Hamburg on September 8, 2019. A "Weiterlesen" button is visible next to the article title. On the right side, there is a section for "Neueste Beiträge" (Latest Contributions) with several article titles listed.

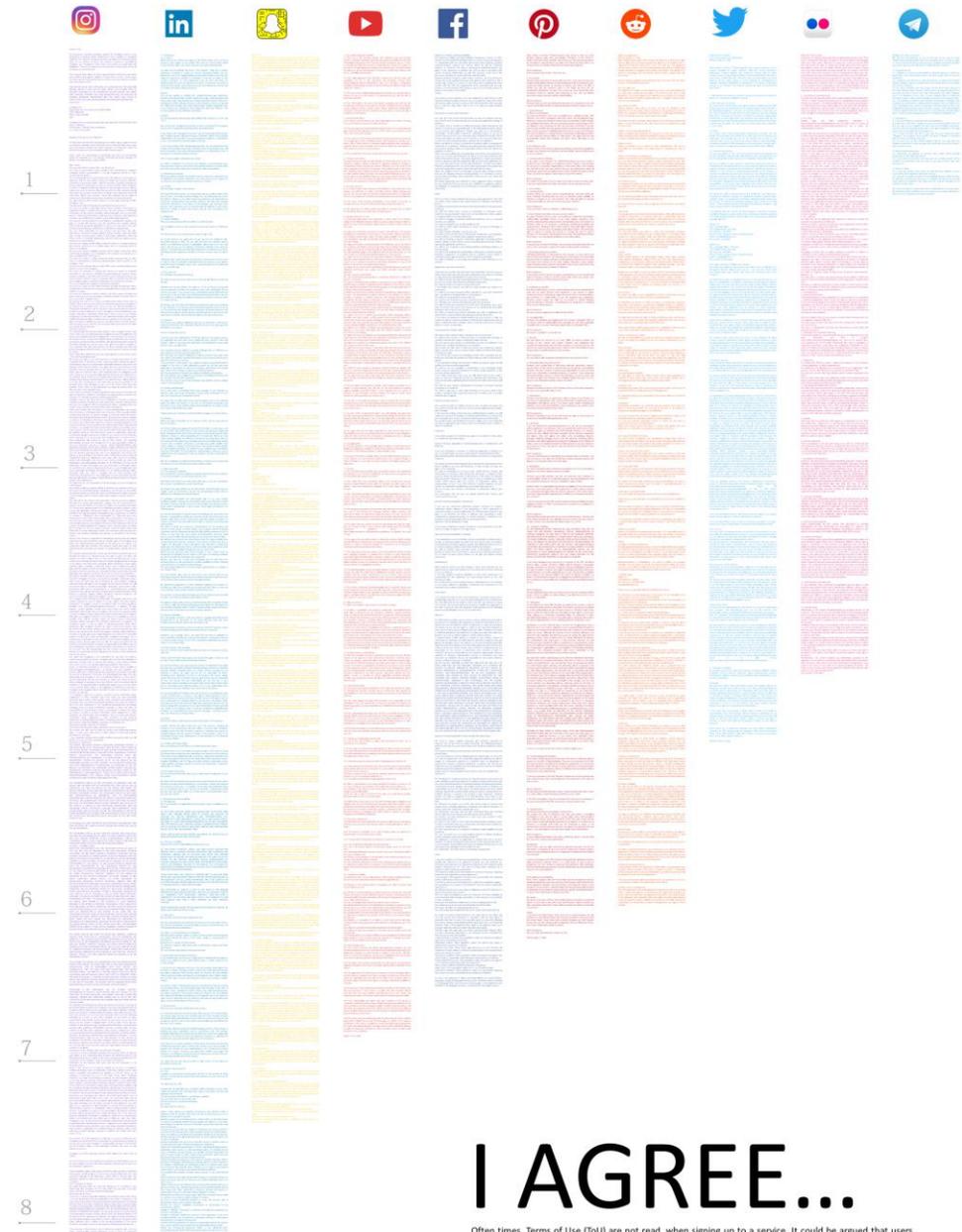


# Woran wir sonst arbeiten

Kontext: Legal Design

Weiterentwicklung Zweckbindungsgrundsatz

- Wie denken Menschen über Datenschutzrisiken nach, wenn sie Daten freigeben?
- Wie wird das Prinzip der Zweckbindung aktuell praktisch umgesetzt?
- Passen diese beiden Konzepte zusammen?
- Was kann eigentlich mit meinen Daten passieren, wenn sie „Zur Verbesserung des Dienstes“ eingesetzt werden?



---

## Woran wir sonst arbeiten

### Privacy Icons

- Nach DSGVO sollen standardisierte und „effektive“ Icons geschaffen werden.
- Viele Vorarbeiten existieren. Neu:
  - Bottom-Up, nutzerzentrierte Perspektive
  - Risiko-basierter Ansatz zu unterschiedlichen Technologien (Sprachassistent, Vernetzte Mobilität)

***Workshops stehen an! Macht mit! :-)***

**[www.privacy-icons.info](http://www.privacy-icons.info)**





---

## DSGVO Kapitel 3, Art.15, Abs.2, Auskunftsrecht der betroffenen Person

- (1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein **Recht auf Auskunft** über diese personenbezogenen Daten [..]
- (3) Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem **gängigen elektronischen Format** zur Verfügung zu stellen [..].

Erwägungsgrund 63:

- 1) [..] **problemlos** und in angemessenen Abständen wahrnehmen können, **um sich der Verarbeitung bewusst zu sein** und deren Rechtmäßigkeit überprüfen zu können.
- 4) **Nach Möglichkeit** sollte der Verantwortliche den **Fernzugang** zu einem sicheren System bereitstellen können, der der betroffenen Person **direkten Zugang** zu ihren personenbezogenen Daten ermöglichen würde



---

## Wie schätzt Du die Umsetzbarkeit der DSGVO für Usability Professionals ein?

- 5 % sehr hohe Unsicherheit
- 37 % hohe Unsicherheit
- 41 % etwas Unsicherheit
- 15 % kaum Unsicherheit
- 2 % keine Unsicherheit

Quelle: German UPA Mitgliederbefragung 2018  
(n = 184)



---

# Musstest Du Lösungen entwickeln bzw. Systeme anpassen, um folgende Anforderungen zu erfüllen?



Recht auf Vergessenwerden (Datenlöschung)

Auskunftsrecht

Recht auf Berichtigung

Recht auf Einschränkung der Verarbeitung

Recht auf Datenübertragbarkeit

Kopplungsverbot („Service gegen Daten“)

Datensparsamkeit

German UPA Mitgliederbefragung 2019  
(Befragung läuft)



---

## DSGVO: Folgen für Usability Professionals & BürgerInnen

- Was sind eure Erfahrungen mit der DSGVO im Arbeitskontext
  - Welche Relevanz hat die DSGVO aktuell in eurer Arbeit?
  - Welche Unterstützungsleistungen werden im Kontext DSGVO angefragt?
  - Wie wird das bisher gelöst in Praxis?
  - Wo gibt es Best Practices/Informationen?
- Welchen Umgang habt ihr bisher mit der DSGVO privat gehabt?
  - Was hat sich für euch privat geändert?
  - Wo habt ihr schon mal eure neuen Rechte ausgeübt?
  - Wo seid ihr wegen der DSGVO an (neue?) Grenzen gestoßen?

Alizadeh, Fatemeh, et al. "GDPR-Realitycheck on the right to access data." *Mensch und Computer 2019-Tagungsband* (2019).



---

## Ergebnisse: Berufliche Erfahrungen mit der DSGVO

- Je nach Aufgabe von wenig bis extreme Relevanz der DSGVO
- Wenig Wissen über konkrete Details und Umsetzung
- Erstellung von Dokumenten zur Zustimmung zur Verarbeitung der Daten (Testpersonen)
- Einrichtung Server: Personenbezogene Daten dürfen nicht offenliegen
- Informationen von Datenbeschutzbeauftragten, Gesetzestexte, Fachzeitschriften (Zeitschrift für Datenschutz), Newsletter
- Im Rahmen der eigenen Masterarbeit
- Kontakt mit DSGVO als wissenschaftlicher Mitarbeiter
- App zur Schulung von Mitarbeitern (Sensibilisierung)
- IP-Adresse wird beim Download getrackt
- Usabilitytest durchführen: informed consent, IP und non-disclosure, Teilnehmer-Anmeldung und Recruiting (Vendor-Einkauf)
- Als Seminarteilnehmer
- Als Datenschutzbeauftragter
- Als Procedure Owner im Verfahrensverzeichnis
- Als Autor von Datenschutzerklärungen



---

## Ergebnisse: Private Erfahrungen mit der DSGVO

- Pop-ups
- Cookie-Hinweise, Cookies auf Websites
- Cookie-Einstellungen als Qualitätsmerkmal, Cookie ablehnen (funktioniert das effektiv überhaupt?)
- Kriterium ist eher Vertrauen in Dienst als Liste der Cookies (denn die werden nicht gelesen)
- Geänderte Datenschutzrichtlinien
- Erklärung, man habe dem Datenschutz-Hinweis "schon zugestimmt"
- Eigene Daten heruntergeladen
- Interesse, "was noch passiert"



---

## Hands-On: Google Takeout

**Selbstversuch und UX Analyse:**  
**Holt Euch Eure Daten!**  
(ohne Youtube, Drive und Fotos)



---

# Ergebnis

## 1. Team:

- nicht leicht zu finden, einfach Google genutzt
- Umweg über E-Mail
- Einstieg über Google Help: Wording "back-up", "multiple formats" (?) für Download

## 2. Team:

- über Google.de - Datenschutzerklärung - Login; anschließend Verifizierung mittels Smartphone
- Reiter "Persönliche Daten" / "Daten & Personalisierung" / "Sicherheit"

## 3. Team:

- Anmeldung bei Google und Einstellungen Datenschutz
- viele Infos
- Daten exportieren schnell gefunden
- Daten herunterladen
- Auswahl von Download und Downloadformat
- Meldung "Jemand möchte deine Daten herunterladen"
- Löschen/Exportieren: sehr lange Liste, einzelne Checkboxen zum Abwählen



---

## Hands-On: Die Zukunft des Google Takeout

<https://takeout.opendash.de>

- Welche Daten sind interessant?
- Welche Visualisierungen wären toll?
- (Datenschutz-)Anforderungen an einen Takeout



---

## Ergebnisse

- Übergreifende Rohdatensammlung in Verbindung mit potenzieller Datenauswertung
- Ggf. Hinweis, wie bzw. wo die Daten verwendet wurden (Download history)
- Direkte Möglichkeit zur einfachen/editierbaren Löschung der Rohdaten
- Angabe von Anzahl/Ort ("von wem")/... getrackt wurde
- Nach Öffnen der ZIP Ladeindikator und automatische Weiterleitung
- Auswahl der Services und Beschreibung des Services
- Hinweise zur Datensparsamkeit mit Link zum Deaktivieren oder Löschen (Privatsphärecheck)
- Takeout für andere Dienste
- Hinweis, dass OSM Cookie gesetzt wird
- Design, Styling



---

**Welche weiteren (insbesondere deutschen)  
Services wären interessant für Takeouts?**



---

# Ergebnisse

- lokale Lebensmittelgeschäfte
- lokale Restaurants, in denen man gegessen hat
- (Online-)Zeitschriften wie Spiegel, Zeit usw.
- Onlinehändler, z. B. otto.de



# Abschlussfrage: Welche weiteren Google Services wären interessant für den Takeout?



**Arts & Culture**  
Favoriten und Galerien.



**Classroom**  
Ihre Classroom-Kurse  
[Weitere Informationen](#)



**Cloud Print**  
Cloud Print-Verlauf und -Geräte.



**Data Shared For Research**  
Mit Ihrem Google-Konto ges  
Fc



**YouTube**  
Wiedergab



**Street View**  
Bilder und



**Assistant Notes and Lists**  
Ihre Notizen und Listen in Go



**Gespeichert**  
Sammlungen g  
Google-Suche u



**Gmail**  
Alle Nachrichten und A  
[Weitere Informationen](#)



**Drive**  
Dateien



**Google Fit**  
Ihre Google Fit-Akti



**G Suite Marketplace**  
Metadaten, die eine in G



**Google Kontak**  
Kontakte und Kc



**Google Groups**  
Alle Google Groups-E



**Google Fotos**  
Ihre Fotos und Videos  
Google+, Blogger und



**Google Input Tools**  
Synchronisierte erlernte



**Google News**  
Daten zu den Zei  
sind.



**Google Shopping**  
Bestellverlauf bei Go



**Beiträge zur Google-Suche**  
Ihre Bewertungen, Rezensionen, Kommentar  
Google-Suche



**Hangouts**  
Ihr Gespräch:



**Notizen**  
Alle in Goo



**Maps (Meine Orte)**  
Datensätze zu Ihren m:



**Kalender**  
Ihre Kalende



**Home App**  
Informationen zu



---

# Ergebnisse

- Kontakte (3 Nennungen)
- Mail (3 Nennungen)
- Google Home (2 Nennungen)
- Kalender (2 Nennungen)
- Assistant (1 Nennung)
- Google Fit (1 Nennung)
- Google Shopping (1 Nennung)
- Hangouts (1 Nennung)
- Notizen (1 Nennung)
- Photos (1 Nennung)
- Youtube (1 Nennung)
- Drive (0 Nennungen)
- Google News (0 Nennungen)

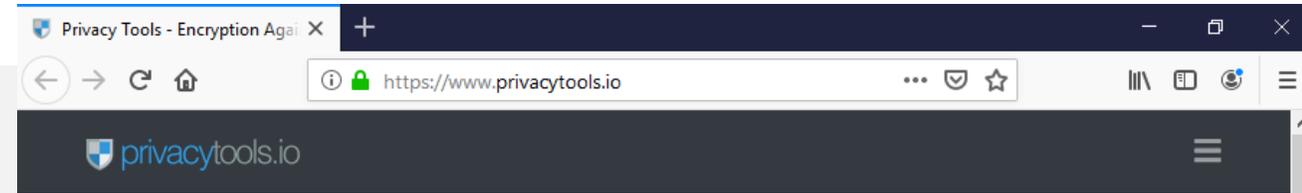


# Wie kann man sich schützen?

PrivacyTools.io

*"Services, tools and knowledge to protect your privacy against global mass surveillance"*

<https://www.privacytools.io/>



You are being watched. Private and state-sponsored organizations are monitoring and recording your online activities. privacytools.io provides services, tools and knowledge to protect your privacy against global mass surveillance.

Try search.privacytools.io, a Privacy-Res

## Privacy Tools

[i Prefer the classic site? View a single-page layout.](#)

Providers

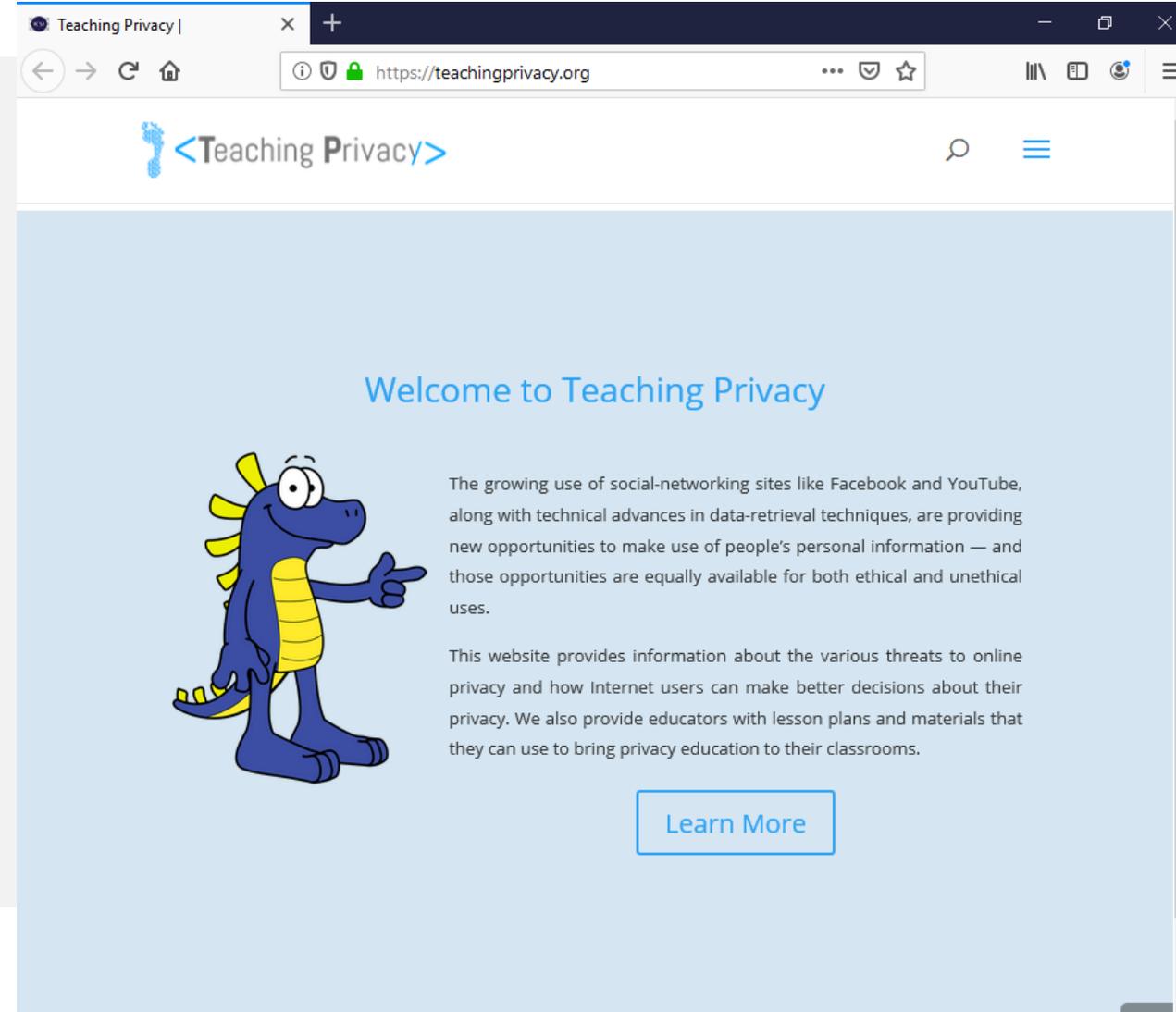


# Wie kann man sich schützen?

TeachingPrivacy.org

*"Information about the various threats to online privacy and how Internet users can make better decisions about their privacy"*

<https://teachingprivacy.org/>





# Wie kann man sich schützen?

## Data Detox Kit

*"The Data Detox Kit's clear suggestions and concrete steps help people harness all aspects of their online lives, making more informed choices and changing their digital habits in ways that suit them."*

<https://datadetoxkit.org>

<https://www.klicksafe.de/themen/data-detox-kit/>

