

LINKS ZUM UMGANG MIT DATENSCHUTZ, FAKE NEWS UND SOCIAL MEDIA

Zusammengestellt für das Werksgespräch 56 am 23.5.18

Grundlegende Medien:

<https://netzpolitik.org>

<https://re-publica.com/de>

http://www.faz.net/aktuell/feuilleton/medien/abschluss-der-re-publica-der-feind-in-meinem-computer-15009370.html?printPagedArticle=true#pageIndex_0

Bericht von der re:publica

<https://digitalcharta.eu/>

Entwurf eines europäischen Grundgesetzes für die digitale Gesellschaft

Datenschutz

DSGVO-Themenportal bei netzpolitik.org:

<https://netzpolitik.org/tag/dsgvo/>

Die Datenschutzgrundverordnung DS-GVO

<https://www.datenschutz-wiki.de/Datenschutz-Grundverordnung>

Der Hamburger Datenschutzbeauftragte

<https://www.datenschutz-hamburg.de/>

Datenschutzinfo der Hamburger Verbraucherzentrale

<https://www.vzhh.de/themen/telefon-internet/datenschutz/ihre-daten-ihre-rechte>

Portal der Wikipedia zu Datenschutz und Informationsfreiheit

https://de.wikipedia.org/wiki/Portal:Datenschutz_und_Informationsfreiheit

Alles über Datenschutz !!!

<https://www.datenschutz-wiki.de/Hauptseite>

Recht am Bild/Fachanwalt Florian Wagenknecht

<https://www.rechtambild.de/2018/05/fotografieren-in-zeiten-der-dsgvo-grosse-panikmache-unangebracht/>

Fake News

Ist diese Meldung seriös oder ein Gerücht? Das klärt der Claimchecker:
<https://claimchecker.de/>

<http://hoax-info.tubit.tu-berlin.de/hoax/>

<https://correctiv.org/projekte/>

<http://faktenfinder.tagesschau.de/>

<https://www.zeit.de/serie/fakt-oder-fake>

außerdem: Online-Auftritte seriöser Medien

Facebook

Facebook-Privatsphäre einstellen:

<http://www.dw.com/de/privatsph%C3%A4re-bei-facebook-was-muss-ich-beachten-was-ist-problematisch/a-43059467>

Rahlstedt-Seite: <https://www.facebook.com/hamburgrahlstedt/>

Rahlstedt-Gruppe: <https://www.facebook.com/groups/rahlstedt>

Sicher Surfen (Aus der Diskussion am 23.5. nachgetragen)

Wer sicher surfen will, muss sich selbst darum kümmern. Das Befolgen der Ratschläge unten verspricht mehr Sicherheit, nicht vollständige Sicherheit.

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/checklisten_node.html
Checkliste des Bundesamtes für Sicherheit im Internet

Wer seine Daten nicht an Google oder Microsoft weitergeben will, kann

1. **Browser** verwenden, die versprechen, anonym zu operieren:
Mozilla Firefox, Cliqz

Dazu muss man die bei Windows standardmäßig vorinstallierten Browser Internet Explorer oder Edge deinstallieren bzw. wenn man sie behalten will, einen anderen Browser herunterladen. Bei dessen Installation wird man gefragt, ob das der Standard-Browser sein soll.

2. **Suchmaschinen** verwenden, die versprechen, anonym zu operieren:

Startpage, duckduckgo, Metager, ixquick

Auch hier sind in neuen Geräten standardmäßig die Suchmaschinen vorinstalliert, die den Big Five gehören, oft auch über „Schnellsuche“ vorinstalliert empfohlen.

Als „Suchmaschinen“ empfohlen/eingerichtet sind auch Shoppingplattformen wie Ebay, amazon, booking.com – alles firmeninterne Werbung und gekaufte Plätze.

3. Als sicherster, aber unter Umständen auch langsamer Browser gilt TOR.

<https://www.torproject.org/projects/torbrowser.html.en>

4. Wer seine Daten schützen will, u.a. vor Google, sollte keine Google-Programme verwenden, als da wären u.a.: Gmail, googlemail, Google maps, Youtube.

5. Regelmäßig Browser und Betriebssystem updaten!

6. Nicht für alle Anwendungen das selbe Passwort verwenden!

Über Sicherheitsfragen im Internet informieren die IT-Berater des KulturWerks Rahlstedt in ihren Newslettern bzw. auf ihrer Homepage:

<http://www.it-suling.de/> Gerlinde Suling

<https://it-kroeger.de/thema/software/> Jens Kröger

Hamburg, 24.5.18 Tobias Gohlis (Mitarbeit: Katharina Thomsen, Willy Theobald)