



Digitale Selbstbestimmung –

Hintergründe und Tipps zum Umgang mit Daten im Netz.



GPA **djp**

GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK - JOURNALISMUS - PAPIER

AutorInnen

© Nurih. Wogner-Strauss



Mag.ª Clara Fritsch

Abteilung Arbeit & Technik der GPA-djp



Hans Christian Voigt

Soziologe und externer Referent für die GPA-djp

Unter Mitarbeit von

Thomas Kreiml

Bildungsabteilung der GPA-djp

Impressum:

Herausgeber: Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier

1030 Wien, Alfred-Dallinger-Platz 1

Redaktion: Vera Kalchgruber MA; GPA-djp Grundlagenabteilung

Layout: GPA-djp Marketing, Ulrike Pesendorfer

Fotos: GPA-djp, fotolia.com

ZVR 576439352

Stand: Jänner 2019

Inhalt

1. Einleitung	5
1.1. Das Digitale – ein wenig Hintergrund	5
1.2. Datenübertragung	7
1.3. Personenbezogene Daten und deren Auswertung	8
2. Sichere Geräte und gesicherte Umgebungen – umsichtiges Verhalten und technische Einstellungen schützen dich	12
2.1. Das Passwort und die Bildschirm-Sperre	12
2.2. Die Software und ihre Updates	13
2.3. Die Internet-Suche und der Browser	13
2.4. Externe Daten	14
2.5. Datensicherheit offline	14
2.6. Verschlüsselung, Zertifizierung und Identitätskontrolle	15
2.7. Datenminimalismus – auch auf Plattformen	17
3. Zusammenfassung	20
4. Spannendes rund um das Thema bietet	20
5. Die Tools im Überblick	21

1. Einleitung

Wir stecken mitten drin in der digitalen Transformation. Auch wenn sich viele immer wieder die Frage stellen, wohin die Reise geht, ist zwischendurch der Blick zurück angebracht. Das letzte Jahr hatte es in Sachen Digitalisierung und Datenschutz in sich. Mit Beginn des Jahres 2018 erhielt Österreich eine *Bundesministerin für Digitalisierung und Wirtschaftsstandort*. Im April 2018 musste der Chef von *Facebook* vor dem Justizausschuss des US-Senats aussagen, weil sein Unternehmen die Daten der NutzerInnen an andere Firmen weitergibt – und etwas später wird er dafür vor das EU-Parlament zitiert. Aus China kommen Meldungen, wonach der staatlich eingeführte *Social Credit Score* bestimmt, welche BürgerInnen welche Leistungen erhalten (z.B. Wohnung, Schulplatz, Krankenbehandlung etc.). In Wien demonstrieren um die tausend Taxi-LenkerInnen gegen den US-Konzern *Uber*, der als Onlineplattform Vermittlungsdienste zur Personenförderung anbietet und dessen FahrerInnen CrowdworkerInnen sind. Seit Mai 2018 ist die *Europäische Datenschutzgrundverordnung* in Kraft. Der ÖGB-Bundeskongress steht im Juni desselben Jahres unter dem Motto *Faire Arbeit 4.0 – vernetzt denken, solidarisch handeln*.

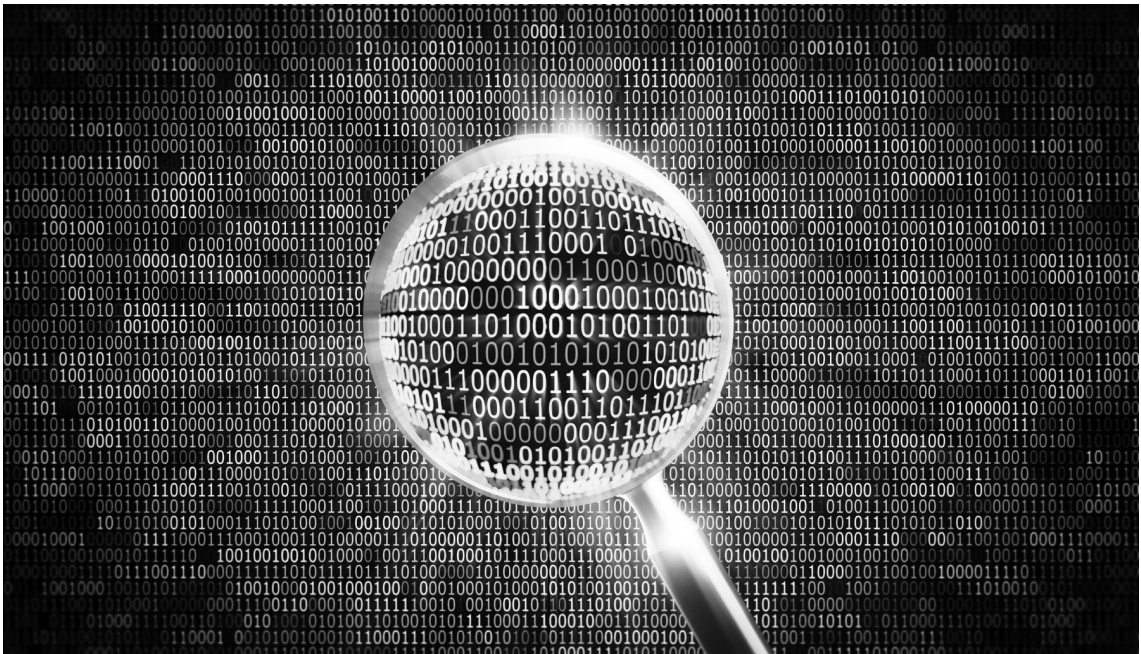
All diese Ereignisse haben miteinander zu tun und sie werfen Fragen auf. Was wird Bestand haben und was sind „Eintagsfliegen“? Welche Chancen eröffnen neue Technologien? Bringen sie Arbeitserleichterung, Informationszuwachs und mehr Beteiligung? Oder bringen sie mehr Überwachung, Vereinsamung und übermäßige Beeinflussung durch einige wenige Konzerne oder Staaten? Kann man sich darauf vorbereiten und sich davor schützen?

Die vorliegende Broschüre der GPA-djp wird nicht die Antwort auf alle Fragen liefern, aber sie wird einige (kleine) Schritte zu mehr *digitaler Selbstbestimmung im Alltag* aufzeigen. Ob in der Betriebsratsarbeit, im Privatleben, als KonsumentIn oder bei der Nutzung von Kommunikationstechnologien: Diese Broschüre soll dazu beitragen, die Risiken besser einschätzen und eindämmen zu können.

Wir fassen Erfahrungen aus Beratungsprozessen und Seminaren zusammen und möchten allen Interessierten damit ein Werkzeug in die Hand geben, um internetbasierte bzw. datenverarbeitende Systeme in höherem Maße selbstbestimmt zu nutzen.

1.1. Das Digitale – ein wenig Hintergrund

Internet, Smartphones, Apps, Big Data und ihre vielen „Verwandten“ gibt es nur, weil es digitale Anwendungen gibt. Im Englischen sind *digits* die Ziffern einer Zahl. Digits sind die kleinsten Bausteine, um zu rechnen, mathematische Funktionen und logische Operationen auszuführen. Im binären Code gibt es nur zwei *digits*, zwei Ziffern. In den zwei Ziffern 0 und 1 lässt sich jeder Wert ausdrücken, der mit den zehn Ziffern des Dezimalsystems dargestellt werden kann. Darüber hinaus lassen sich ebenso Schriftzeichen, Rechenzeichen, Buchstaben in den gleichen reduzierten Binärcode übersetzen. 0 oder 1 kann für einen von zwei möglichen Zuständen stehen, für keine elektrische Ladung (0) oder elektrische Ladung (1). 0 und 1 können somit auch als Signal verwendet werden. Null oder Eins, ja oder nein, richtig oder falsch, EIN oder AUS, entweder oder. Darstellungen von Welten aus Nullen und Einsen verdeutlichen heutzutage diese binäre Struktur.



Um in diesen binären Strukturen schnell rechnen zu können, braucht es die elektronische Datenverarbeitung mittels Computer. Mit Computer finden digitale Daten zugleich schnellere und weitere Verbreitung. Schon seit einigen Jahren hat die Menge an in digitaler Form gespeicherten Informationen jene überholt, die sich im Laufe der Geschichte in Büchern, Gemälden, Schallplatten oder alten Fotografien angesammelt hat. Das, was in analogen Speichermedien erhalten ist, wird zunehmend digitalisiert. Dieser Vorgang, bei dem Information aus „alten“ Speichermedien in die Datenformate des Binärcodes kopiert werden, wird – vor allem im englischen Sprachraum – als „Digitalisierung“ bezeichnet.

Digitale Daten können im Gegensatz zu analog gespeicherten einfach, schnell, billig und ohne Informationsverlust kopiert werden. Beim Kopieren eines gedruckten Buches, einer analogen Fotografie, einer Schallplattenaufnahme, gibt es unvermeidbar einen gewissen Informationsverlust. Das Kopieren von Nullen und Einsen schafft dagegen zwei idente Kopien im Binärcode. Original und Kopie sind gleichwertig.

Wesentlicher noch als die Einfachheit des Speicherns beliebig vieler Kopien ist, dass digitale Daten beliebig verknüpft werden können. Über Hyperlinks wird Information in neue Zusammenhänge gebracht. Websites werden miteinander verlinkt, Texte nehmen aufeinander Bezug und Websites speichern, was verlinkt ist und werten es aus. Zu gewünschten Informationen werden Links verschickt. Im Fotoprotokoll einer Sitzung oder eines Workshops verweisen Links zu Dokumenten wie PDFs oder zu virtuellen Ordnern. Ordner können sich sowohl innerhalb der Firmen-Infrastruktur befinden als auch an externen Speicherorten bei Fremdanbietern, also in der sogenannten „Cloud“. In Social Media wird mit Bezug zu Online-Zeitungen oder anderen Informationsquellen diskutiert. Werbung, aber auch politische Aussagen werden personalisiert und dorthin verlinkt, wo per Auswertung des Nutzungsverhaltens Zielgruppen ausgemacht werden.



WAS HEISST EIGENTLICH DIGITAL?

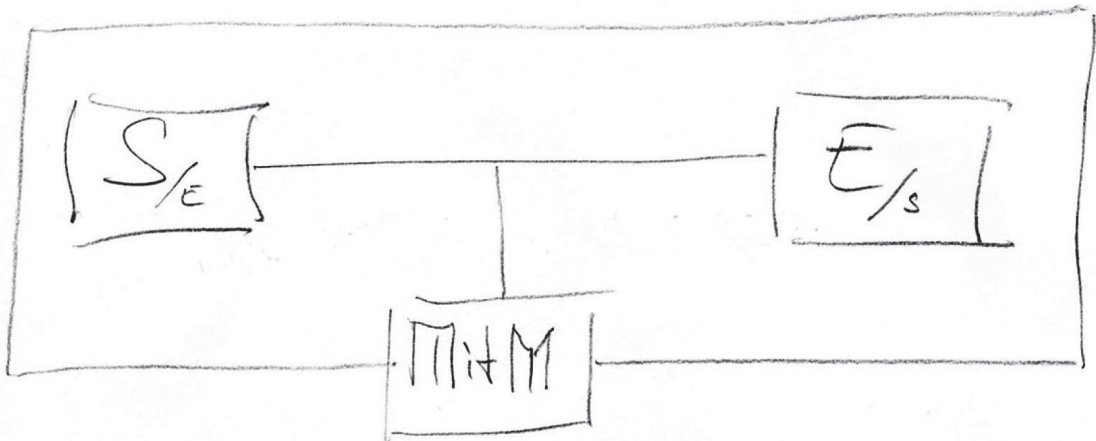
Der Kern des Digitalen sind die Nullen und Einser als kleinste Bausteine der Information. Informationen sind somit einfacher kopier- und speicherbar, schnell übertrag- und verknüpfbar. Unter Digitalisierung wird das automatisierte Erfassen, Kopieren, Verknüpfen, Auswerten und Speichern von Daten verstanden.

1.2. Datenübertragung

Digitale Kommunikation ist immer mit Datenübertragung verbunden. (Mobile) Geräte senden und empfangen (z.B. um Kommunikation und Standortbestimmung zu ermöglichen). Das Navigationsgerät im Auto, die Bankomatkarte, der Chip zum Eintritt in den Betrieb, die e-card beim Arzt oder der Ärztin - in jedem dieser Fälle werden Daten bzw. Datenpakete übertragen.

Bei der digitalen Datenübertragung werden die Bits aber nicht direkt von dem/der SenderIn zu dem/der EmpfängerIn transportiert, wie dies bei einer analogen Ansichtskarte der Fall wäre. Die Datenübertragung erfolgt über Zwischenstationen. Auf dem Weg, den die Datenübertragung nimmt, fallen aller Wahrscheinlichkeit nach Kopien an, die dann bei AnbieterInnen, DienstleisterInnen, auf Rechnern, in Sicherungssystemen und Arbeitsspeichern landen können. Oftmals ist nicht klar, ob diese Kopien erhalten bleiben oder gelöscht werden. Aber selbst wenn sie als gelöscht gelten, stellt sich die Frage, *ob* sie sicher und überall gelöscht sind und *wo* sie angefallen sind und – zumindest zwischenzeitlich – gespeichert waren. Hinzu kommt, dass sich bei vielen Datenübertragungen am Weg „ein Dritter“ einschaltet. Für diese Dritten, die leicht unbemerkt bleiben können, hat sich der Begriff „Man in the Middle“ (MitM) etabliert.

Schematische Darstellung des Sender-Empfänger-Systems der Datenübertragung



Quelle: Christian Voigt, CC

Der „Man in the Middle“ lässt SenderInnen und EmpfängerInnen glauben, sie würden miteinander kommunizieren, während sich in Wirklichkeit der zwischengeschaltete „Man in the Middle“ als SenderIn bzw. EmpfängerIn ausgibt. (*Phishing* nennt man es, wenn es um Websites geht, auf die Dritte in Täuschungsabsicht umleiten wollen.) MitM können aber auch ganze Systeme umprogrammieren oder eigene Programme installieren. Diese wiederum könnten im worst-case die technische Infrastruktur übernehmen. Dann spricht man von MitM-Attacken.

Um ungestört und ohne MitM zu kommunizieren, sind einige Maßnahmen hilfreich:

- *Daten verschlüsselt übertragen:* NutzerInnen können zwar nicht verhindern, dass Provider, Server oder heimlich zwischengeschaltete Dritte unsere Datenpakete kopieren und speichern. Dass Inhalte mitgelesen werden, kann aber verhindert werden. Dazu gibt es Verschlüsselungssoftware. Ein Email ist Klartext und daher mit der Postkarte zu vergleichen. Eine Verschlüsselung macht aus dem von jedem lesbaren Klartext der Postkarten ein verschlossenes Kuvert (→ derzeit aktuell empfohlene Software siehe Seite 15)
- *Digitale Signatur prüfen:* Um festzustellen, ob KommunikationspartnerInnen diejenigen sind, für die sie sich ausgeben, dient die digitale Signatur. Dabei wird ein persönlicher Schlüssel (z.B. der der eigenen IP-Adresse) mit einem öffentlichen Schlüssel (z.B. dem der angesurften Webseite) verglichen und geprüft (→ wie das geht, steht auf S. 15).
- *Die eigenen Geräte vor ungewolltem Zugriff schützen:* Dabei helfen Passwörter (→ zur Gestaltung von Passwörtern siehe S. 12), Virenschutz-Programme und Spamfilter.



WIE KANN ICH DEN „MAN IN THE MIDDLE“ VERMEIDEN?

Der MitM schleicht sich unbemerkt bei der Datenübertragung ein und täuscht vor, der/die jeweilige SenderIn/EmpfängerIn zu sein. So erfolgen die meisten Hackerangriffe, Virenattacken, Betriebsspionagefälle etc. Ungestörte digitale Kommunikation basiert auf Verschlüsselung, Überprüfung der Identität von SenderIn und EmpfängerIn sowie dem Schutz der Geräte vor ungewolltem Zugriff.

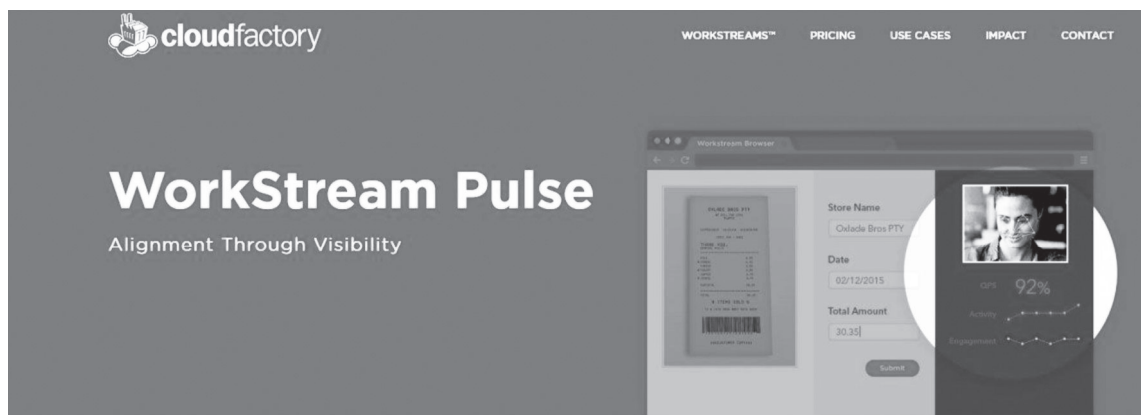
1.3. Personenbezogene Daten und deren Auswertung

Ob bei digitaler Kommunikation, Navigation im Fahrzeug, Arbeit am Computer oder an der Produktionsmaschine: immerzu fallen sogenannte „Metadaten“ an. Diese „Metadaten“ sagen nichts darüber aus, was an Inhalten übertragen wird, jedoch jede Menge darüber wie übertragen wird. Verbindungsdaten, wie Zeitstempel, Standortbestimmung, Verbrauchsangaben an Maschinen etc. können Auskunft darüber geben *wer wann wo und wie lange* gearbeitet hat. Die Daten sind ursprünglich nicht unbedingt personenbezogen, können aber indirekt Personen zugeordnet werden.

Durch Auswahl und Einstellung der technischen Systeme und Geräte kann in einem Unternehmen festgestellt werden, von wem, wann, welche Daten(-sätze) produziert werden.

Diese Metadaten sind für manche Unternehmen selbst zum Geschäftsmodell geworden. Beispielsweise bietet das Unternehmen „Cloud Factory“ an, Projekt-Teams, LeiharbeiterInnen und ProjektleiterInnen optimal zu rekrutieren, indem sämtliche Aktivitäten der Beschäftigten – und derer die es werden wollen – ausgewertet werden. Cloud-Factory arbeitet mit selbstlernenden Algorithmen, um die Produktivität der Teams sowie die Produktqualität vorherzusagen. „Sie können die Gesundheit der Beschäftigten in Echtzeit erfassen sowie die Produktivität ihres Teams. (...) Ergänzend nutzen wir Webcams um das Engagement-Level jedes Arbeiters zu messen.“¹ wirbt das Unternehmen.

Beispiel für betriebliche Überwachungsszenarien



Activity & Engagement Monitoring

By tracking key data points from our WorkStream Browser, we gather important metrics on workforce activity such as keystrokes and time spent on the resources used to complete tasks. In addition, we utilize each computer's webcam to measure the level of engagement of each worker.



Quelle: <https://www.cloudfactory.com/workstream/pulse>

Die Metainformationen können zu Persönlichkeitsprofilen verdichtet werden. Diese Profile sagen bisweilen mehr über eine Person aus, als diese eigentlich bereit wäre, über sich preiszugeben. Beim herangezogenen Datenmaterial ist nicht immer ganz klar, woraus es besteht, wie es gesammelt wurde und ob es berechtigt im Besitz der Unternehmen ist. Mit den Daten aus den Profilen wird dann hochgerechnet, wie eine Person(-engruppe) sich aller Wahrscheinlichkeit nach zukünftig verhalten wird und eine Abstufung wird festgelegt. In der digitalen Welt spricht man hier von *Scoring*; in Anlehnung an eine Punktebewertung im Sport.

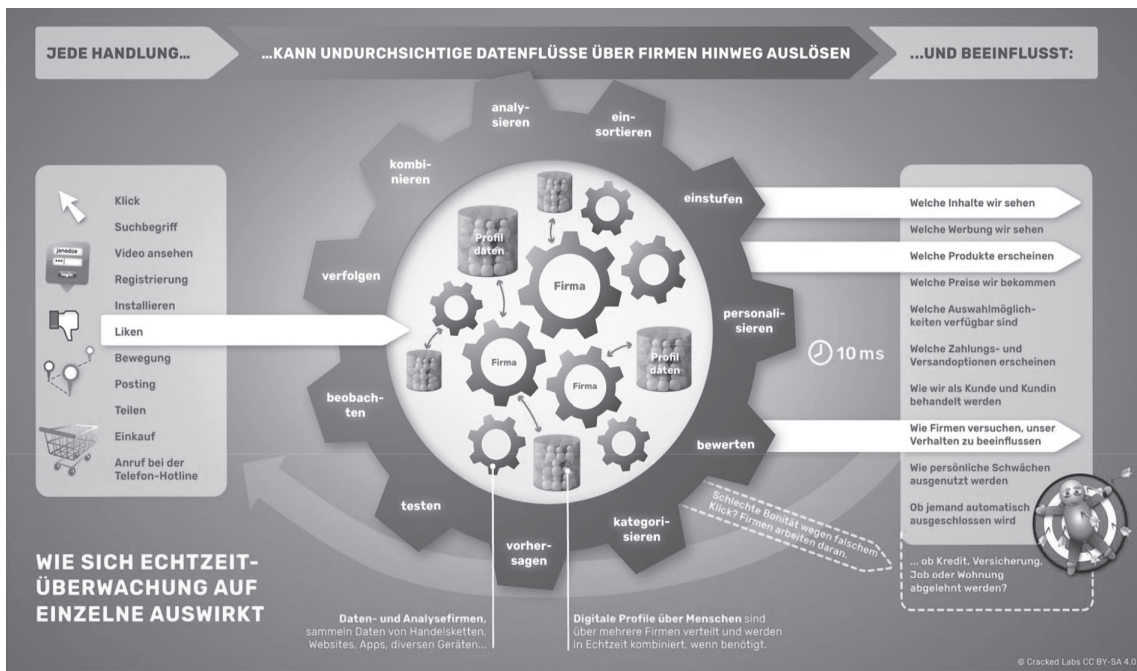
¹ Quelle: <https://www.cloudfactory.com/workstream> [09.01.2019]

In der Finanzwelt gibt der Kreditscore beispielsweise Auskunft, ob Personen wahrscheinlich einen Kredit zurückzahlen werden – oder nicht. Die Entscheidung obliegt dann dem Wahrscheinlichkeitsmodell.

Nicht nur die Produktivität der ArbeitnehmerInnenschaft oder Kreditwürdigkeit wird auf diese Weise vorhersagend berechnet. (Sogenannte „predictive analytics“ werden auch unter dem Begriff *Big Data* subsummiert.) Es gibt auch Unternehmen, die Produkte anbieten, die weitreichende Vorhersagen zur Arbeitsplatzsicherheit treffen. Die Firma „Workday“ bietet Software an, die die Wahrscheinlichkeit für Kündigungen berechnet. Der Europäische CEO erklärt im Interview: „Unsere Software braucht 1,5 Jahre Datenhistorie der Firma, dann spuckt unser Algorithmus die Abwanderungswahrscheinlichkeit zu 93 Prozent richtig aus.“²

Bei *Profiling und Scoring* ist allerdings in Zukunft mit einigen rechtlichen Problemen zu rechnen. Außerdem untersagt die Europäische Datenschutzgrundverordnung derartige Praktiken generell – soweit die Betroffenen nicht zugestimmt haben.

Schematische Darstellung der Inhalte und Auswirkungen von Echtzeitüberwachung



Quelle: CC BYSA Cracked Labs, 2017

2 <http://www.business-punk.com/2016/06/workday-software/> [09.01.2019]



WAS PASSIERT EIGENTLICH MIT MEINEN META-DATEN?

Daten, die im Internet oft nur als „Nebenprodukt“ und ohne direkten Personenbezug entstehen, können zu Profilen verdichtet werden, die wiederum zur Bewertung von Personen dienen sollen. Geschäftsmodelle milliardenschwerer Industrien bestehen im Datensammeln, Datenbewertung, Daten kaufen und verkaufen.



FAQ

WAS KANN ICH TUN?

- Nur die Pflichtangaben auf Plattformen bereitstellen (diese sind bei Onlineformularen üblicherweise mit einem * gekennzeichnet);
- Privatsphäre-Einstellungen auf Plattformen nutzen und restriktiv einstellen, sodass möglichst wenige Menschen mitlesen können;
- Ad-Blocker installieren (Siehe S. 18);
- auf Browser und Programme bzw. Apps beschränken, bei denen „tracking“ minimiert werden kann (z.B. Signal statt WhatsApp, Mozilla Firefox statt Microsoft Internet Explorer oder Edge; (siehe Kapitel 5);
- den Tor-Browser nutzen (siehe S. 15);
- Datenauskunfts- und Löschrechte (gemäß Europäischer Datenschutzgrundverordnung ³) in Anspruch nehmen;
- Self-tracking Apps wie z.B. runastic, Apple Health vermeiden;

Datenschutz- und Konsumentenschutzorganisationen unterstützen: ihre Newsletter abonnieren, an ihren Aktionen beteiligen, ihre Info-Materialien weiterverbreiten, ihre Finanzierung mit einer Spende unterstützen.

³ Für detaillierte Informationen zur Europäischen Datenschutzgrundverordnung (EU-DSGVO) siehe die GPA-djp Broschüre „Die europäische Datenschutzgrundverordnung aus ArbeitnehmerInnen-Sicht“ (Mai 2018)

2. SICHERE GERÄTE UND GESICHERTE UMGEBUNGEN – UMSICHTIGES VERHALTEN UND TECHNISCHE EINSTELLUNGEN SCHÜTZEN DICH

2.1. Das Passwort und die Bildschirm-Sperre

Zuallererst sollte sichergestellt sein, dass kein Gerät ohne *Anmeldung* verwendet werden kann. Die Anmeldung läuft üblicherweise über einen Benutzernamen und ein *Passwort*. Bei der Erstellung eines Passwortes gilt grundsätzlich: je länger und komplexer, desto sicherer. Die Verwendung von Groß- und Kleinbuchstaben in Kombination mit Ziffern erhöht die Komplexität eines Passwortes. Ein Passwort, das kürzer als zwölf Zeichen ist, entspricht nicht mehr den heutigen technischen Standards, und sollte daher vermieden werden. Heutzutage sollte der/die umsichtige NutzerIn *Passphrasen* oder *Passsätze* bilden. Ein kurzer Satz hat schnell die Länge von zwanzig Stellen – damit ist man „auf der sicheren Seite“. Sätze bieten darüber hinaus Groß- und Kleinbuchstaben sowie Satz- bzw. Sonderzeichen. Sätze finden sich außerdem leicht auf analogen Medien gespeichert (z.B. in einem der Bücher, Broschüren, Rechtstexte etc., die im Betriebsratsbüro im Regal stehen).

Sind viele ZugangsCodes, Passwörter und -phrasen zu merken, bietet sich die Nutzung eines *Passwort-Managers* an. Das sind Programme, in denen Codes gespeichert werden können, die mit einem einzelnen, besonders komplexen, *Master-Passwort* verschlüsselt und geschützt sind. Wird eine Passphrase gebraucht, muss der Passwort-Manager geöffnet werden. Der dazu benötigte Code ist der einzige, den man sich auswendig merken muss. Alle anderen sind digital gespeichert mit einem Klick kopiert und mit dem nächsten dort eingefügt, wo es gerade gebraucht wird.

Biometrische Anmeldeverfahren, wie sie immer wieder von Apple für iPhones und iPads angepriesen werden, sollten – außer vielleicht für Bereiche der Hochsicherheit – vermieden werden. Ein biometrisches Merkmal ist einerseits völlig einmalig (eben, weil es nur einer einzigen Person zugeordnet werden kann) und zugleich nur sehr schwer abänderbar (zumindest nur durch größere körperliche Eingriffe). Sollte ein solches Merkmal in die falschen Hände geraten, kann das unangenehme Folgen haben.

Neben der Qualität von Passwörtern ist die Einstellung, dass bereits nach wenigen Minuten der Inaktivität eines Gerätes eine *erneute Anmeldung* erforderlich ist, ein weiterer Sicherheitsaspekt. Bildschirmschoner bzw. die grundlegenden Einstellungen des Geräts helfen, um nach ein oder zwei Minuten der Inaktivität die Zugangsabfrage zu erzwingen. Zusätzlich sorgt so das Sperren des Bildschirms per Tastenkombination beim Verlassen des Raumes für mehr Sicherheit. (Bei Windows-Geräten genügt die Kombination aus *Windowstaste* und *L* für „lock“, zu Deutsch *verschießen*.)

Neben dem Gerät selbst, sollten die sich darauf befindlichen sensibleren Bereiche, Ordner, Festplatten-Partitionen (das sind Unterteilungen der Festplatte in unterschiedliche Bereiche) mit Passwörtern gesichert werden. Das ist umso wichtiger, wenn auch andere Zugang zum Gerät haben. Geht ein Gerät verloren oder wird es gestohlen, sollten die Daten nicht auslesbar sein. Ein Gerät bzw. die Festplatte eines Geräts kann auch zur Gänze verschlüsselt werden. Bei mobilen Geräten ist dies jedenfalls zu empfehlen. Anbieter von Smartphones bieten diese Option in der Regel heute schon an.

Eingeschaltete Geräte haben die Verschlüsselung der Festplatte mit dem Betriebssystem notwendigerweise deaktiviert, weil sie sonst nicht laufen könnten. Mobile Geräte sollte man deshalb nicht permanent aktiviert lassen. Sie *herunterzufahren* ist eine weitere Schutzmaßnahme gegen ungewollten Zugriff.

2.2. Die Software und ihre Updates

Software-Updates sind ein Aspekt, um mit Geräten und Umgebungen möglichst sicher umzugehen. In aller Regel schließen Software-Updates Sicherheitslücken, daher empfiehlt es sich, Updates besser gleich als später zu installieren. Nach Möglichkeit empfiehlt es sich auch *freie Software* nutzen. Beispielsweise kann hier *Linux* als Betriebssystem dienen. *Libre Office* deckt die Funktionalität des Microsoft Office ab.

Vor der Installation einer Software sollte jedenfalls die *Signatur* des abgespeicherten Datenpakets geprüft werden. Dabei muss man das Schloss-Symbol in der Titelzeile der Suchmaschine anklicken. Dort wird das Prüfzertifikat und die Prüfende Organisation bzw. Institution dargestellt. Man erfährt, ob ein Zertifikat vorliegt und wie lange es gültig ist.

Einen Unterschied macht zudem, *wo man sich Software herunterlädt*. Am besten macht man das auf der Website der Hersteller und nicht auf Plattformen, die massenhaft Downloads anbieten. Wer es genau nimmt, lädt Software dann außerdem verschlüsselt herunter.

Unbekannte Programme sollten nicht blindlings heruntergeladen, installiert und ausgeführt werden. Etwas Recherche im Netz, was andere zur Sicherheit der jeweiligen Anwendung zu berichten wissen, ist gut investierte Zeit. Bei Wikipedia und bei Datenschutz-NGOs (z.B. www.epicenter.works) gibt es immer wieder aktuelle Informationen, von welcher Software abgeraten und welche empfohlen wird. Software, die irgendwann zu einem Anlass installiert wurde und abgesehen vom diesem einen Anlass nicht gebraucht wird, sollte auch wieder *deinstalliert* werden.

2.3. Die Internet-Suche und der Browser

In jedem Fall zahlt es sich aus, alternative Suchmaschinen zu benutzen (z.B. Startpage.com oder duckduckgo.com). Diese erstellen keine (Hintergrund-)Profile ihrer NutzerInnen, erheben keine zusätzlichen Daten (wie etwa Standorte) und gelten generell als Privatsphäre-freundlicher als die großen Internet-Riesen. (Zu den „Big Four“, den großen Vier, hat sich die Abkürzung GAFa etabliert, sie steht für: Google, Apple, Facebook, Amazon).

Der *Firefox-Browser* ist aktuell der beste, schnellste und sicherste Browser. Ein Browser verdient besondere Aufmerksamkeit und kann je nach Einstellungen und Erweiterungen sehr unterschiedlich konfiguriert werden. (Siehe dazu auch Kapitel 5)

2.4. Externe Daten

Dass mitgeschickte Dateien und Programme, so genannte „Anhänge“ bzw. „Attachments“ nicht unbedacht angeklickt und ausgeführt werden sollten, hat sich weitestgehend herumgesprochen. Ebenso verhält es sich bei *USB-Sticks* und *externen Festplatten*. An die eigenen Geräte sollten nur die eigenen Geräte angesteckt werden. Die eigenen externen Speicher steckt man dementsprechend auch nicht bei fremden Geräten an. Daten gehen immer wieder verloren. *Backups* auf externen Speichermedien sollten für diese Fälle vorsorgen.

2.5. Datensicherheit offline

Doch auch beim nicht-digitalen Handeln können Sicherheitslücken entstehen. In den letzten Jahren haben besonders „*Brutal-force-Angriffe*“ für Aufsehen gesorgt. Dabei sind einfache Anrufe von Hackern der erste Eingriff in firmeninterne Systeme. Wenn sich also jemand am Telefon oder per Messenger als „Kollege aus der IT-Abteilung“ oder „beauftragte Sicherheitsexpertin“ vorstellt, um die Überprüfung von ein paar Einstellungen bittet und dafür um ein Passwort ersucht, dann sollten die Alarmglocken laut läuten und die Identität des Gegenübers genau überprüft werden.



WAS IST DAS WICHTIGSTE FÜR DIE SICHERHEIT IM INTERNET?

Das Um und Auf für (technische) Sicherheit ist der Schutz der Geräte vor ungewollten Zugriffen. Dieser kann mittels technischer Maßnahmen gewährleistet werden, aber auch „analoge Vorsicht“ kann dazu beitragen.



FAQ

WAS KANN ICH TUN?

- „Pass-Sätze“ statt Pass-Wörter verwenden;
- alternative Suchmaschinen (z.B. Startpage.com) und Browser (z.B. Firefox) verwenden;
- recherchieren, was aktuell empfehlenswerte Software ist und wovor gewarnt wird;
- nach Möglichkeit Open Source- und freie Software nutzen;
- die Kommunikationsmittel des Betriebsrats sollten vor ungewolltem Zugriff gesichert sein: das kann entweder in der technischen Infrastruktur des Unternehmens erfolgen oder der Betriebsrat arbeitet mit eigenen, vom Unternehmen unabhängigen Geräten und Speicherplätzen.

2.6. Verschlüsselung, Zertifizierung und Identitätskontrolle

Es gibt Kommunikationsmittel, die sich nicht verschlüsseln lassen (z.B. SMS). Es gibt Kommunikationsmittel, die verschlüsselt werden können, bei denen das aber etwas aufwendig ist (z.B. Email). Es gibt Kommunikationskanäle, die sowohl unverschlüsselte als auch verschlüsselte Datenübertragung kennen (z.B. das Surfen im Internet).

Ein Blick auf die Webadresse gibt an, ob verschlüsselt wurde oder nicht. Steht im Feld des Browsers eine einfache Adresse (<http://www...>), dann ist die Kommunikation unverschlüsselt. Steht <https://> (das „s“ steht für secure) im Suchfeld und links davon das Symbol eines Vorhängeschlosses, dann werden die Datenpakete zwischen Browser und Server der Website verschlüsselt übertragen.

Dabei geht es aber um mehr als nur um verschlüsselte Datenpakete. Hinter dem System steckt zusätzlich die Überprüfung auf Richtigkeit, der Check, ob tatsächlich mit einer echten Website Daten ausgetauscht werden. Diese Überprüfung wird von Organisationen aus der ganzen Welt vorgenommen, die als *Zertifikatsaussteller* tätig sind. Sie zertifizieren die Verschlüsselungsalgorithmen von Webseiten und überprüfen, wer hinter Websites steht, um dem Browser grünes Licht für die weitere Kommunikation zu geben.

Soll die Zertifizierung nicht über Dritte oder eigene Organisationen erfolgen, sondern direkt von Sender zu Empfänger, bietet sich *Pretty Good Privacy* (pgp) an. Pretty Good Privacy (pgp) ist seit drei Jahrzehnten ein System, das ziemlich gut für die Privatsphäre funktioniert. Geheimdienste können das System bis heute nicht knacken und es steht allen als freie Software zur Verfügung. Die Schattenseite ist, dass das Verschlüsseln auf eigene Verantwortung sehr aufwendig ist.

Es gibt auch Kanäle, die von sich aus *Verschlüsselung garantieren* (z.B. Tor-Browser, die Nachrichten-App Signal). *Tor* steht für *The Onion Router*. Es handelt sich um eine spezielle Anpassung des Firefox Browsers, der verschlüsselte Verbindungen zu Webseiten über mehrere Zwischenstationen führt. Die Umleitung der Datenpakete erfolgt über zufällig ausgewählte Pfade. Der Tor-Server anonymisiert beim Surfen. Es können aufgerufene Websites nicht erfassen, wer surft, weil die eigene IP-Adresse durch eine zufällige aus dem Tor-Netzwerk ersetzt wird. Und der Provider kann nicht erkennen, wer surft, weil auch hier eine zufällige IP-Adresse angezeigt wird (siehe Kapitel 5).

In den letzten Jahren ist eine gute Alternative für *Instant-Messaging* inklusive Austausch von Bild- und Tonaufnahmen entwickelt worden. Mit der App *Signal* werden Nachrichten verschlüsselt übertragen und man kann sogar verschlüsselt VOIP-Telefonie nutzen.⁴

Außerdem lassen sich Dateien, Dateiordner oder Laufwerke verschiedentlich verschlüsseln. Der *Leseschutz für Microsoft Office Dateien* ist wohl die am häufigsten eingesetzte Möglichkeit, Dateien zu verschlüsseln.

⁴ Welche Messenger-Apps derzeit noch empfehlenswert sind, steht in diesem Artikel der Süddeutschen Zeitung: <https://www.sueddeutsche.de/digital/smartphone-apps-diese-messenger-sind-sicherer-als-verschluesselte-emails-1.3978888> (21.12.2018)

Zur Verschlüsselung größerer Datenmengen wird derzeit die freie Software *VeraCrypt* empfohlen. Damit werden nicht einzelne Dateien, sondern virtuelle Ordner bzw. Laufwerke verschlüsselt, in denen Dateien dann vor dem Zugriff Unbefugter geschützt sind. (Siehe auch Kapitel 5)



KANN ICH MEINE KOMMUNIKATION VERSCHLÜSSELN?

Verschlüsselung sollte Standard für den Umgang mit Information sein. Beim Surfen im Internet, der Festplatten-Verschlüsselung, der Verschlüsselung von Mobilgeräten und bei einigen Messenger-Diensten gibt es dazu bereits datenschutzfreundliche Möglichkeiten.



FAQ

WAS KANN ICH TUN?

- Microsoft-Dateien mit Leseschutz ausstatten;
- beim Surfen im Internet immer auf https-Seiten zugreifen;
- verschlüsselte Email-Kommunikation funktioniert, ist aber eher aufwendig durchzuführen und daher selten – daher alternativ Informationen in verschlüsselten Anhängen versenden;
- verschlüsselte Chats oder Messenger-Apps nutzen (z.B. Signal);
- Email-Adressen nicht bei Google oder den anderen großen Anbietern kostenloser Email-Accounts anlegen: es gibt kleine Anbieter, die auf Datenschutz, grüne Energie, vertrauensvolle Beziehungen zwischen Anbieter und KundInnen setzen und ihre Server in Europa stehen haben ⁵;
- den Tor-Browser verwenden;
- VeraCrypt verwenden.

5 Im österreichischen Konsumentenschutz-Magazin erzielten 2017 die Anbieter „Mailbox“ (<https://mailbox.org/>) und „Posteo“ (<https://posteo.de/de>) beispielsweise recht gute Testergebnisse. (<https://www.konsument.at/emailedienste022017> [letzter Zugriff: aktuelles Datum einfügen!])

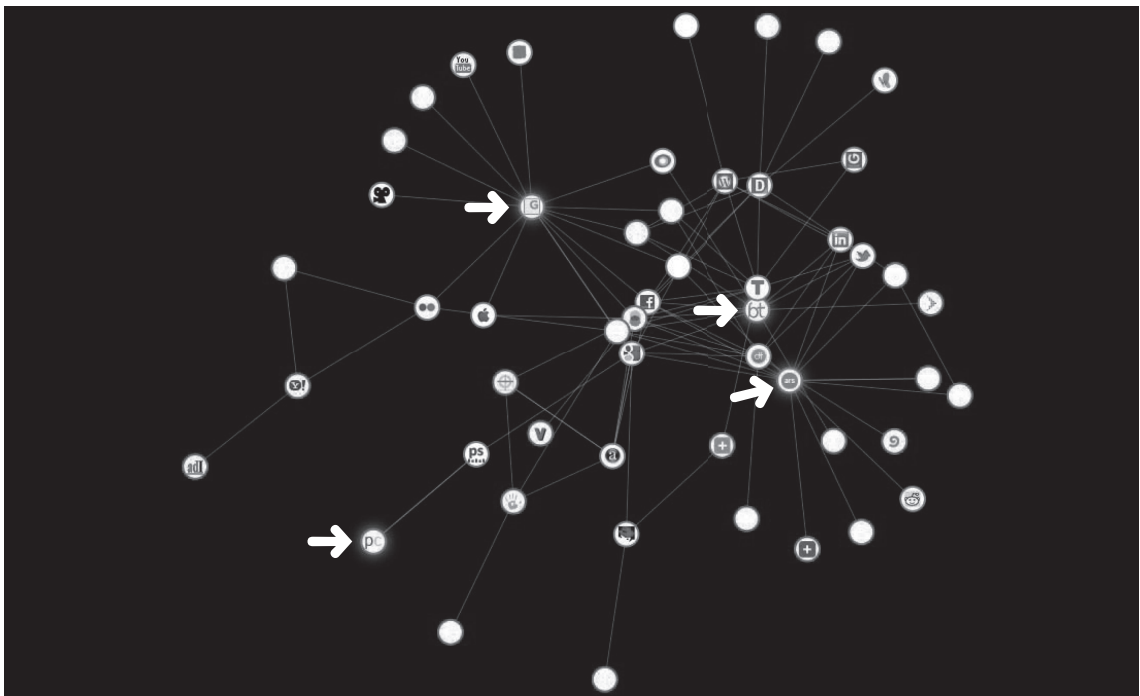
2.7. Datenminimalismus – auch auf Plattformen

Zusätzlich zu dem, was NutzerInnen ohnehin selbst an Daten zur Verfügung stellen, haben Internet-Plattformen zahlreiche weitere Informationen über ihre NutzerInnen. Auch wer große Kommunikationsplattformen wie Facebook oder Google gar nicht nutzt, ist deshalb noch lange kein/e Unbekannte/r für diese Konzerne. Erstens gelingt es den Plattformen von Kontakten, die die Plattformen nutzen, auch auf jene zu schließen, die sie nicht nutzen – sie legen sogenannte *Schattenprofile* an.

Diese werden aus Daten erstellt, die über den Umweg anderer NutzerInnen gewonnen werden und mit denen auf Wohnort, Bildungsstationen, ArbeitgeberIn, Familienmitglieder, Kaufkraft usw. hochgerechnet wird. Zweitens liefern UserInnen schon beim Surfen oder einer App-Nutzung Daten an die – oft unmerklich – dahinterstehenden Unternehmen. Unternehmen sind auf Websites oft unsichtbar anwesend – wenn die sichtbaren WebsitebetreiberInnen ihnen dazu Rechte einräumen. Diese Dritten sind für Werbung verantwortlich, für eingebettete Funktionen zur Optimierung der Website, zur statistischen Auswertung oder Weiterleitung auf andere Plattformen. In vielen Fällen ist ihr Geschäft das *Tracking* von Website-BesucherInnen.

Für den Browser Firefox gibt es einige *Erweiterungen (Add-Ons)*, mit denen solche unsichtbaren Dritten sichtbar gemacht werden und es gibt Erweiterungen, mit denen sie ausgeschaltet werden können. Eindrucksvoll visualisieren lassen sich die Drittanbieter mit der Mozilla-Erweiterung *Lightbeam*.

Lightbeam im Einsatz:



Quelle: Wikipedia, CC By 2.0

Die vier mit einem Pfeil gekennzeichneten Kreise sind unmittelbar besuchte Websites. Die anderen Kreise sind Websites, die nur durch Cookies mit dem Browser verbunden sind, darunter bekannte Datensammler.

Werbungsblocker wie *uBlock Origin*⁶ und tracking-Blocker wie der *Privacy-Badger* minimieren erfolgreich, wie viele Informationen über uns an Dritte gelangen und bestimmen auch, an welche Dritte Informationen weitergereicht werden. (siehe auch Kapitel 5)



WIE KANN ICH IM INTERNET MEINE PRIVATSPHÄRE MÖGLICHST GUT SCHÜTZEN?

Um möglichst wenige personenbezogene Daten im Internet preiszugeben, ist die Internetnutzung ein weites Übungsfeld. Das betrifft sowohl die Auswahl der Websites (https!), als auch die Browser und Apps, mit denen man surft. Die werksmäßige Standardeinstellung ist meist ungenügend.

Browser und mobile Geräte können so eingestellt werden, dass man kaum Daten an Dritte liefert. Suchmaschinen müssen nicht zwangsläufig unsere Suchbegriffe erfassen (Mozilla) und auch auf Plattformen wie Facebook stehen restriktive Einstellungen zur Verfügung. Empfehlungen für all diese Aspekte finden sich im WorldWideWeb gut aufbereitet und aktuell, was es sehr erleichtert, up-to-date zu bleiben.

⁶ <https://addons.mozilla.org/de/firefox/addon/ublock-origin/> [09.01.2019]

WAS KANN ICH TUN?

Für Plattform-Accounts weder die private Email-Adresse noch die der Firma verwenden, sondern eigene, die nur für die Verwaltung der Plattform-Accounts genutzt werden und keine Adressbücher mit Kontakten enthalten.

„**Cookies**“ sind kleine „Hinterlassenschaften“ von den Betreibern der Seite auf dem eigenen Computer, die das Verhalten im Internet registrieren. Sie machen einmal besuchte Seiten leichter wieder auffindbar, verfolgen dazu aber auch das gesamte Surfverhalten. Es gibt mehrere Möglichkeiten im Umgang mit Cookies:

- Man lässt sie wo sie sind, damit man die eigene Suchgeschichte nachvollziehen kann.
- Man löscht sie selbst immer wieder händisch, damit man nicht von Werbung und anderen unliebsamen Seiten verfolgt wird. Das funktioniert indem man das Symbol „Einstellungen“, meist ein Zahnrad, und dort den Begriff „Sicherheit“ anklickt. Bei den meisten Browsern gibt es dann die Möglichkeit „den Browserverlauf löschen“.
- Man ändert die Browsereinstellungen, sodass von Haus aus keine Cookies zugelassen werden, was allerdings langwierig werden kann, weil man sich mitunter durch viele Möglichkeiten durchklicken muss. Meist findet sich aber auch dazu etwas unter dem Symbol des Zahnrades.
- Man lädt sich aus dem Internet Software herunter, die jegliche Cookies (oder andere Zugriffe Dritter) sperrt. Damit ist Tracking (also das Nachverfolgen im Internet) weitgehend verhindert. Derzeit wird dafür der „*Privacy Badger*“ in Datenschutz-Kreisen empfohlen.

Für das Recherchieren im Netz eignen sich alternative Suchmaschinen (z.B. *Startpage.com*, *DuckDuckGo.com*). Sie speichern Suchbegriffe nicht und verdichten sie auch nicht zu persönlichen Suchprofilen, wie das Google, Bing oder Yahoo tun. (siehe auch Kapitel 5)

3. Zusammenfassung

Das Internet und die darin stattfindende Kommunikation sind aus dem Leben nicht mehr wegzu-denken. Komfort, Wissen, Information und Unabhängigkeit sind genauso enthalten wie Überwa-chungspotenzial, Beeinflussung und wirtschaftliche Vorteile für einige wenige Konzerne. Doch wo ein Mittel, da ein Gegenmittel und so finden sich auch zahlreiche größere und kleinere Mittel und Wege, den nicht gewollten Aspekten – zumindest teilweise – zu entkommen.

All das gibt es „im Netz“ und ist oft didaktisch gut aufgebaut. Kompetenz in den Einstellungen von Browsern und Smartphones, in der Auswahl von Add-Ons und Apps kommt nicht von heute auf morgen. Es erfordert Geduld und Zeit. Eine Empfehlung unsererseits: halbjährlich die Suchmaschinen anwerfen und nach den aktuellen Empfehlungen der DatenschützerInnen und SicherheitsexpertInnen suchen; besonders instruktiv und vielfach sehr gut aufbereitet sind hier auch Videos, z.B. auf YouTu-be. Es zahlt sich aus, diesen Quellen zu folgen und den einen oder anderen Tipp auszuprobieren. Regelmäßiges Durchführen derartiger Recherchen führt zum einen zu mehr eigener Sicherheit, zum anderen aber auch zu der unbedingt erforderlichen Aktualität. Es ändert sich mitunter sehr schnell, was gerade als Empfehlung gilt. Es kann sich auch rasch ändern, welches Add-On, welche Soft-ware nicht mehr weiterentwickelt wird, während sich andere neue Ansätze durchsetzen.

4. Spannendes rund um das Thema bietet

Die **Abteilung für Konsumentenschutz der Arbeiterkammer Wien** hat immer aktuelle Informationen zum Datenschutz für KonsumentInnen:

<https://wien.arbeiterkammer.at/beratung/konsumentenschutz/datenschutz/index.html>

Die Seite des **ÖGB** zum Kongress 2018 inklusive einem umfassenden Digitalisierungs-Glossar:

<https://www.arbeitfairgestalten.at/>

Die von Unterrichtsministerium und EU co-finanzierte Organisation „**Safer Internet**“ hat gut aufberei-tete Materialien für Kinder, Jugendliche, PädagogInnen und SeniorInnen zum Verhalten im Internet: <https://www.saferinternet.at/>

Die international tätige NGO „**epicenter.works**“ hat zahlreiche hilfreiche Vorschläge zur digitalen Selbstverteidigung zusammengetragen: <https://epicenter.works/crypto>

Der **ChaosComputerClub Berlin** betreibt ein wiki mit „Anleitungen zur digitalen Selbstverteidigung“ – sehr empfehlenswert! https://berlin.ccc.de/wiki/Digitale_Selbstverteidigung/Surfen

Einfach am Ball bleiben, was sich im Internet so tut:

<https://netzpolitik.org/>

<https://digitalcourage.de/>

...und last but not least sei den LeserInnen im Bezug auf Datenschutz und Arbeitsverhältnis der Blog der Abteilung Arbeit & Technik ans Herz gelegt: <http://arbeitundtechnik.gpa-djp.at/>

5. Die Tools im Überblick

ADD-ONS // BROWSER-ERWEITERUNGEN



uBlock Origin

uBlock Origin ist eine Browser-Erweiterung, die kostenlos ist und deren Quelle öffentlich einsehbar und veränderbar (= „Open-Source“) ist.

Blockiert und schützt damit vor ungewollter Werbung.



Privacy Badger

Der Privacy Badger ist eine weitere Browser-Erweiterung, die den/die NutzerIn vor ungewolltem Tracking schützt. Diese Plugin verhindert, dass man beim Surfen im Web websiteübergreifend verfolgt wird.

Entwickelt von EFF – Electronic Frontier Foundation, einer internationalen Non-Profit-Organisation für digitale Rechte.



Https Everywhere

Eine weitere kostenlose, open-source Browser-Erweiterung. Entwickelt von EFF, gemeinsam mit The Tor Project (eine Non-Profit-Organisation, die u.a. den Tor-Browser entwickelt hat).

Die Erweiterung leitet die/den UserIn automatisch an die sichere, verschlüsselte Verbindung der Website weiter, wenn es eine solche gibt.

ALTERNATIVE SUCHMASCHINEN

[Startpage.com](https://www.startpage.com)

StartPage

StartPage gehört zu den datenschutzfreundlichen Suchmaschinen. Die Suchanfrage wird an die Google-Suchmaschine weitergeleitet und gibt deren Ergebnisse zurück, dies geschieht aber anonymisiert. StartPage steht quasi als schützendes Schild zwischen dem/der UserIn und Google.

Nach eigenen Angaben werden weder IP-Adressen noch Cookies gespeichert. IxQuick und StartPage gehören seit 2016 zusammen.



DuckDuckGo

DuckDuckGo

Auch DuckDuckGo betont den Schutz der Privatsphäre der NutzerInnen und vermeidet damit das Entstehen einer Filterblase, wie sie durch die Speicherung der Suchanfragen bei Google entsteht. DuckDuckGo brüstet sich damit, dass die Suchmaschine allen NutzerInnen dasselbe Ergebnis zeigt und nicht mit personalisierten Ergebnissen arbeitet. Dafür werden zwar die Suchbegriffe gespeichert, aber weder die IP-Adresse noch werden Cookies verwendet.

DATEIEN VERSCHLÜSSELN



VeraCrypt

Zum Verschlüsseln der Daten auf Notebooks und externen Festplatten wird die quelloffene Software Veracrypt empfohlen.

Was genau das Programm kann und wie man es installiert, ist beispielsweise hier erklärt: <https://www.lehrerfreund.de/schule/1s/anleitung-veracrypt/4807>

ALTERNATIVE MESSENGER-DIENSTE



Signal

Epicenter.Works empfehlen Signal als eine sichere Messaging Alternative zu SMS, WhatsApp und Telegram.

Die App kann beinahe alles, was auch WhatsApp kann: Bilder, Dateien, Videos und vieles mehr kann mit diesem Messenger sicher und verschlüsselt geteilt werden. Dabei sind nicht nur die Inhalte verschlüsselt wie bei WhatsApp, sondern auch die Metadaten der Kommunikation.

ALTERNATIVE BROWSER



Mozilla Firefox

Firefox ist ein kostenloser, quelloffener Browser.

Dieser Browser lässt sich über unzählige Plugins, also Erweiterungen, anpassen und noch sicherer machen (bspw. Werbeblocker, Tracking-Schutz etc.).

Wie Firefox konfiguriert werden kann, steht hier: <https://keepmydesktop.blog/2018/03/16/firefox-quantum-add-ons-datenschutz/>



Tor

= The Onion Router

Die Verbindung zu Webseiten läuft darin über mehrere Zwischenstationen, die zufällig ausgewählt werden. Dies anonymisiert das Surfen im Web, da nicht mehr erkennbar ist, woher die Anfrage kam – es wird die eigene IP-Adresse durch eine zufällig ausgewählte IP-Adresse aus dem Tor-Netzwerk ersetzt.

<https://www.torproject.org/>

GPA-djp BROSCHÜREN

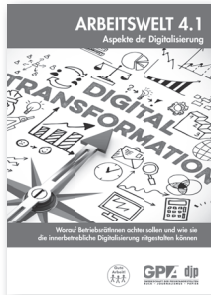


Anywhere working

Irgendwie - irgendwo - irgendwann

Zur Gestaltung mobiler Arbeit

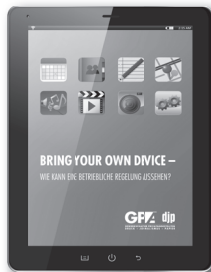
Wien: August 2018. Broschüre der GPA-djp.



Arbeitswelt 4.1 Aspekte der Digitalisierung

Worauf BetriebsrätInnen achten sollen und wie sie die innerbetriebliche Digitalisierung mitgestalten können.

Wien: Mai 2018. Broschüre der GPA-djp.



Bring your own device (BYOD)

Wie kann eine betriebliche Regelung aussehen?

Wien: November 2013. Broschüre der GPA-djp



Sozial? Digital? Oder von beidem ein bisschen?

Personalentwicklung in der digitalen Arbeitswelt.

Wien: März 2017. Broschüre der GPA-djp.

DATENSCHUTZINFORMATION (online unter: www.oegb.at/datenschutz)

Der Schutz Ihrer persönlichen Daten ist uns ein besonderes Anliegen. In dieser Datenschutzerklärung informieren wir Sie über die wichtigsten Aspekte der Datenverarbeitung im Rahmen der Mitgliederverwaltung. Eine umfassende Information, wie der Österreichische Gewerkschaftsbund (ÖGB)/Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier (GPA-djp) mit Ihren personenbezogenen Daten umgeht, finden Sie unter www.oegb.at/datenschutz.

Verantwortlicher für die Verarbeitung Ihrer Daten ist der Österreichische Gewerkschaftsbund. Wir verarbeiten die uns von Ihnen angegebenen Daten mit hoher Vertraulichkeit, nur für Zwecke der Mitgliederverwaltung der Gewerkschaft und für die Dauer Ihrer Mitgliedschaft bzw. solange noch Ansprüche aus der Mitgliedschaft bestehen können. Rechtliche Basis der Datenverarbeitung ist Ihre Mitgliedschaft im ÖGB/GPA-djp; soweit Sie dem Betriebsabzug zugestimmt haben, Ihre Einwilligung zur Verarbeitung der dafür zusätzlich erforderlichen Daten.

Die Datenverarbeitung erfolgt durch den ÖGB/GPA-djp selbst oder durch von diesem vertraglich beauftragte und kontrollierte Auftragsverarbeiter. Eine sonstige Weitergabe der Daten an Dritte erfolgt nicht oder nur mit Ihrer ausdrücklichen Zustimmung. Die Datenverarbeitung erfolgt ausschließlich im EU-Inland.

Ihnen stehen gegenüber dem ÖGB/GPA-djp in Bezug auf die Verarbeitung Ihrer personenbezogenen Daten die Rechte auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung zu.

Gegen eine Ihrer Ansicht nach unzulässige Verarbeitung Ihrer Daten können Sie jederzeit eine Beschwerde an die österreichische Datenschutzbehörde (www.dsb.gv.at) als Aufsichtsstelle erheben.

Sie erreichen uns über folgende Kontaktdaten:

GPA-djp

1030 Wien, Alfred-Dallinger-Platz 1
Tel.: +43 (0)5 0301-301
E-Mail: service@gpa-djp.at

Österreichischer Gewerkschaftsbund

1020 Wien, Johann-Böhm-Platz 1
Tel.: +43 (0)1 534 44-0
E-Mail: oegb@oegb.at

Unseren Datenschutzbeauftragten erreichen Sie unter:
datenschutzbeauftragter@oegb.at.

MITMACHEN – MITREDEN – MITBESTIMMEN



Interessengemeinschaften der GPA-djp bringen Menschen mit ähnlichen Berufsmerkmalen zusammen. Zum Austauschen von Erfahrungen und Wissen, zum Diskutieren von Problemen, zum Suchen kompetenter Lösungen, zum Durchsetzen gemeinsamer beruflicher Interessen.

Mit Ihrer persönlichen Eintragung in eine oder mehrere berufliche Interessengemeinschaften

>> erhalten Sie mittels Newsletter (elektronisch oder brieflich) regelmäßig Informationen über Anliegen, Aktivitäten und Einladungen für Ihre Berufsgruppe;

>> können Sie Ihre beruflichen Interessen auf direktem Weg in die Kollektivvertragsverhandlungen Ihres Branchenbereichs einbringen;

>> erschließen Sie sich Mitwirkungsmöglichkeiten an Projekten, Bildungsveranstaltungen, Kampagnen, Internet-Foren und anderen für Ihre Berufsgruppe maßgeschneiderten Veranstaltungen, auch auf regionaler Ebene;

>> nehmen Sie von der Interessengemeinschaft entwickelte berufsspezifische Dienstleistungen und Produkte in Anspruch (Fachberatung auf regionaler Ebene, Bücher, Broschüren und andere Materialien);

>> beteiligen Sie sich an demokratischen Direktwahlen Ihrer beruflichen Vertretung auf Bundesebene sowie regionaler Ebene und nehmen dadurch Einfluss auf die gewerkschaftliche Meinungsbildung und Entscheidung.

Nähere Infos dazu unter: www.gpa-djp.at/interesse

Ich möchte mich in folgende Interessengemeinschaften eintragen:

- IG PROFESSIONAL IG FLEX IG SOCIAL IG EDUCATION IG MIGRATION
 IG EXTERNAL IG IT IG POINT-OF-SALE

Dieses Service ist für mich kostenlos und kann jederzeit von mir widerrufen werden.

Frau Herr Titel

Familienname Vorname

Straße/Haus-Nr. PLZ/Wohnort

Berufsbezeichnung Betrieb

Telefonisch erreichbar eMail

.....
Datum/Unterschrift

Ihre Kontaktadressen der **GPA-djp**

Service-Hotline: 05 0301-301

GPA-djp Service-Center

1030 Wien, Alfred-Dallinger-Platz 1

Fax: 05 0301-300, eMail: service@gpa-djp.at

Regionalgeschäftsstelle Wien

1030 Wien, Alfred-Dallinger-Platz 1

Regionalgeschäftsstelle Niederösterreich

3100 St. Pölten, Gewerkschaftsplatz 1

Regionalgeschäftsstelle Burgenland

7000 Eisenstadt, Wiener Straße 7

Regionalgeschäftsstelle Steiermark

8020 Graz, Karl-Morre-Straße 32

Regionalgeschäftsstelle Kärnten

9020 Klagenfurt, Bahnhofstraße 44/4

Regionalgeschäftsstelle Oberösterreich

4020 Linz, Volksgartenstraße 40

Regionalgeschäftsstelle Salzburg

5020 Salzburg, Markus-Sittikus-Straße 10

Regionalgeschäftsstelle Tirol

6020 Innsbruck, Südtiroler Platz 14-16

Regionalgeschäftsstelle Vorarlberg

6900 Bregenz, Reutegasse 11

www.gpa-djp.at

GPA **djp**

GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK - JOURNALISMUS - PAPIER