Data-Dance

Datenschutz-Elektropunk? Klingt merkwürdig, gibt es aber wirklich. *Systemabsturz* heißt das Berliner Duo, welches sich diesem ungewöhnlichen Genre verschrieben hat. Nach eigenen Angaben sind sie gleichzeitig die beste und schlechteste Band ihres Fachs – allerdings ist nur wenig darüber bekannt, wie viel Konkurrenz sie in ihrer Sparte tatsächlich haben. Immerhin aber liefern sie den Beweis dafür, dass Datenschutz tanzbar ist!

Schnapp dir ein paar Kopfhörer, klick auf den Link, oder gib den Titel *Daten, daten, Daten* auf *YouTube* ein und pack die besten Dance-Moves aus, zu denen du heute in der Lage bist:

youtube.com/watch?v=Zc8MF_SWKG0

Wenn Du ausgiebig und ausgelassen deinen ersten Data Dance gedanced hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen!

Datenscham

Hast du Grund zu Datenscham? Oder bist du bereits ein echter Privacy-Ninja? *netzpolitik.org* hat – zum Zwecke eines hauseigenen Spendenaufrufes – einen Datenschamrechner entwickelt, mit dem du anhand von 10 kurzen Fragen deinen persönlichen Privacy-Score ermitteln kannst. Damit wirst du, ob nun mit oder ohne Spende, für Datenschutz und IT-Sicherheit sensibilisiert. Begib dich auf datenscham.org, um deinen eigenen Privacy-Score zu errechnen. Anschließend solltest du dir noch die Auswertung der einzelnen Fragen anschauen – keine Sorge, wirklich schämen brauchst du dich für deine Ergebnisse natürlich nicht.

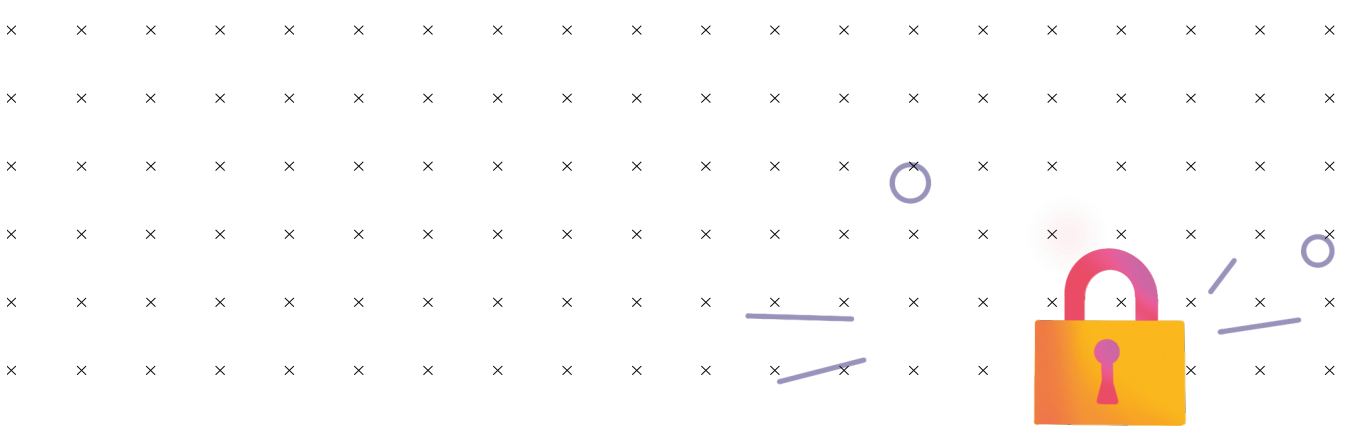
Mit deinem persönlichen Privacy-Score im Gepäck, hast du dir den Seepferdchen-Punkt dieser Station mehr als verdient!

Kryptische Fernmeldung: von Ende zu Ende ohne lose Enden

Sichere, datensparsame E-Mail-Kommunikation fängt bei der Wahl des Anbieters an. Kostenlose Anbieter wie beispielsweise *Googlemail* sind zwar unentgeldlich nutzbar, ihre Dienste bezahlst du aber im Grunde mit dem Verlust deiner Privatsphäre und deinen Daten. Anbieter wie *mailbox.org* und *posteo.de* kosten dahingegend zwar etwas Geld, sind aber im Hinblick auf Datenschutz, Werbefreiheit und sogar auch Nachhaltigkeit die bessere Wahl.
Viele dieser E-Mail Anbieter bieten bezüglich der Datensicherheit sehr komfortable Lösungen. Bei *Posteo* zum Beispiel kann man per Klick alle Mails und Adressen so verschlüsseln, dass sie selbst vom Anbieter nicht mehr eingesehen werden können. Auch gibt es die Möglichkeit, eine sogenannte *TSL*-Garantie (*TSL* steht für *Transport Layer Security*) zu aktivieren, die sicherstellt, dass die Mail nur mit Hilfe dieser Verschlüsselung verschickt wird. Das bietet deiner E-Mail schon einen recht guten Schutz auf dem Transportweg.
TSL ist aber leider auch nicht der Weisheit letzter Schluss. Eine *Ende-zu-Ende-Verschlüsselung*, wie man es von manchen Messengern kennt, bietet *TSL* nicht. *Ende-zu-Ende-Verschlüsselung* bedeutet, dass wirklich nur der Absender und Empfänger die Nachricht entschlüsseln können. Auch für die Kommunikation per E-Mail kann so etwas eingerichtet werden – doch dafür musst du über die Möglichkeiten eines gutes E-Mail Anbieters hinaus selbst aktiv werden. In diesem – schon etwas in die Tage gekommenen, aber immer noch informativen – Video erfährst du die Grundprinzipien dafür:

https://vimeo.com/17610424

Um das alles in die Tat umzusetzen, braucht es ein bisschen Ruhe, Recherche und Zeit, dem man sich auch nach dem Seepferdchenabzeichen widmen kann. Aber wenn du bis hierhin gelesen und wahrscheinlich auch das Video angesehen hast, kannst du dir schon einen Punkt in deinem Seepferdchen-Pass gönnen!



Der heilige Gral

Die Sicherheit deiner E-Mail-Adresse hat im Hinblick auf den Schutz deiner persönlichen Daten oberste Priorität – denn meist laufen dort alle Stränge zusammen. Häufig lassen sich Passwörter, die in den sozialen Medien oder für andere digitale Dienstleistungen verwendet werden, über einen E-Mail-Account zurücksetzen. Der Zugang dazu ist deswegen so etwas wie ein heiliger Gral. Es empfiehlt sich daher, ein separates E-Mail Postfach zu haben, welches du nur zur Registrierung und zum Anlegen für Accounts, aber nicht zur Kommunikation benutzt. So ist diese Adresse im Idealfall niemandem außer dir bekannt. Außerdem solltest du natürlich ein einzigartiges Passwort benutzen und deinen Account mit einer Zwei-Faktor-Authentifizierung absichern. Was das ist und wieso das wichtig ist, erklärt dir die Station mit dem merkwürdigen Namen *qwertz*. Tatsächlich kommt es immer wieder vor, dass es Angreifer:innen gelingt, Datensätze von E-Mail Anbieter:innen zu erbeuten. Vielen Menschen ist oft gar nicht mehr bewusst, wo die eigene E-Mail-Adresse überall hinterlegt ist. Eine Spiele-App, eine Ahnenforschungswebsite, ein Carsharing-Anbieter, eine Datingplattform – die E-Mail-Adresse ist schnell ins Anmeldeformular eingegeben. Das Problem ist, dass bei jedem dieser Anbieter Daten auch verloren gehen können. Das kann durch Fahrlässigkeit der Plattform-Betreiber:innen, aber auch durch ausgeklügelte Hacking-Angriff geschehen. Um herauszufinden, ob persönliche Daten von dir erbeutet worden sind, kannst du dieses Tool des *Hasso-Plattner-Instituts* benutzen:

https://sec.hpi.de/ilc/search?

Wenn Du den Text oben gelesen und eventuell die Sicherheit deiner Mail-Adresse überprüft hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen!

Anonyme Datenschutzsünder:innen

Datenschutz ist zumeist ein Problem des inneren Schweinehunds. Oft wissen wir, dass die Art und Weise, wie wir mit unseren Daten im digitalen Raum umgehen, eigentlich nicht optimal ist, ändern aber trotzdem nichts. Und weil Einsicht oft der erste Schritt zur Besserung ist, haben wir diese Beichtstelle für anynome Datenschutzsünder:innen eingerichtet. Vergeben werden müssen deine Sünden zwar nicht, aber vielleicht steigt deine Motivation, dich zu Besserung zu geloben, wenn du dich hier verewigt hast.

Nachdem du dich eingetragen hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen

„Ich klicke bei Cookies oft einfach auf ›Akzeptieren‹.“

„Ich bin auf *Facebook*, obwohl ich weiß, dass es datenschutzrechtlich schwierig ist!“

qwertz

„qwertz“, also die ersten 6 Zeichen der obersten Buchstabenreihe deiner Tastatur, ist kein sicheres Passwort. Oft scheitert die Passwortsicherheit an der eigenen Faulheit oder Kreativität. Dabei sind gute Passwörter die einfachste und zugleich wichtigste Maßnahme, die du für die Sicherheit deiner Daten ergreifen kannst. In diesem Video erfährst du, worauf du beim Erstellen eines Passwortes unbedingt achten solltest:

https://www.youtube.com/watch?v=cqE1djdxipc

Eine gute Möglichkeit, deine Passwörter zu verwalten, sind digitale Passwortmanager. Diese Programme erlauben es dir, alle Passwörter in einem Dienst abzuspeichern und abzurufen. So musst du dir im Grunde nur ein Passwort merken, nämlich das für den Passwort-Manager.

Eine weitere wichtige Maßnahme ist es, wichtige Zugänge mit der sogenannten *Zwei-Faktor-Authentifizierung* abzusichern. Das kann zum Beispiel eine SMS auf dein Handy sein, durch die dir ein Code zugeschickt wird, den du zusätzlich zu deinem Passwort eingeben musst. Diese Maßnahme sichert meist durch Wissen (dein Passwort) und Besitz (in diesem Fall dein Handy) deinen Zugang ab, bezieht also zwei Faktoren ein und ist entsprechend sicherer.

Wenn du verstanden hast, warum du nie mehr „qwertz“ oder ähnliche Passwörter festlegen solltest, kannst du dir passwortfrei ein Seepferdchen in deinen Ausweis stempeln!

Von Füchsen und Zwiebeln

Dein Browser ist dein Tor zum World Wide Web. Mit jedem Schritt, den du innerhalb von diesem machst, hinterlässt du in jenem einen digitalen Fußabdruck. Sobald du das Internet betrittst, versammeln sich in deinem Browser daher die Unternehmen, die deine Aktivitäten im Internet tracken (wollen) und eröffnen einen kleinen Marktplatz. Der Schutz des Browsers ist deswegen eine der wichtigsten Maßnahmen, um dem Tracking deiner Daten entgegenzuwirken.

Wie sich manch eine:r vielleicht schon denkt, sind die gängigen Browser wie *Google Chrome*, *Microsoft Edge* oder *Safari* keine besonders datenschutzfreundlichen Fortbewegungsmittel. Da *Googles Chrome* von den Werbeeinnahmen lebt, welche der Browser mit den Daten seiner Nutzer:innen macht, verwendet er entsprechend viele Tracking Cookies. Auch *Edge*, der Browser von *Microsoft* behält sich in seinen Datenschutzeinstellungen das Recht vor, Daten an Dritte weiterzugeben. Sowohl *Microsoft* als auch *Apple* sind laut Edward Snowden außerdem Teil des *PRISM*-Überwachungsprogramms, welches Daten direkt an die *NSA* weitergibt.

Eine datenschutzfreundliche und funktionale Alternative ist *Mozilla Firefox*: Keiner der anderen großen Browser achtet so sehr auf Datenschutz wie *Firefox*. Außerdem wurde *Firefox* von der gemeinnützigen *Mozilla Foundation* entwickelt, ist also nicht darauf ausgelegt, möglichst viele Daten von dir zu ergattern, um sie an Werbetreibende zu verkaufen. Zudem ist *Firefox* ein *Open-Source*-Projekt – d. h. dass der Quelltext der Software für jeden zugänglich veröffentlicht ist und unabhängig kontrolliert werden kann. Auch in puncto Plugins (mehr dazu erfährst du bei der Station „Browser-Tuning“) kann *Firefox* punkten.

Wer die maximale Datenschutzerfahrung will, kann auch noch einen Schritt weitergehen und auf einen sogenannten Privacy-Browser zurückgreifen. Der wohl bekannteste und von Edward Snowden 2017 auf *Twitter* empfohlene Browser ist *Tor*, kurz für *The Onion Router*. Wenn du dich damit mit dem Internet verbindest, geschieht das durch das sogenannte *Tor*-Netzwerk – ein Netzwerk an Servern. Wenn du in *Tor* eine Website ansteuern willst, geschieht das über eine zufällige Route, die dich über mehrere Server des *Tor*-Netzwerks zum Ziel führt. Am Ende ist nicht mehr zurückzuverfolgen, wo der Startpunkt war, die IP-Adressse des Computers, mit dem du dich eingewählt hast, bleibt also anonym. Wer sich für einen solchen Privacy- Browser entscheidet, muss allerdings damit rechnen, beim Surf-Komfort einige Abstriche zu machen. Hier gilt es gut zwischen Sicherheit und Funktionalität abzuwägen.

Wenn du bis hierhin gelesen hast und dich in Zukunft vorzugsweise mit Hilfe von Füchsen und Zwiebeln ins Internet begeben willst, kannst du dich mit einem Stempel in deinem Seepferdchen-Pass belohnen!

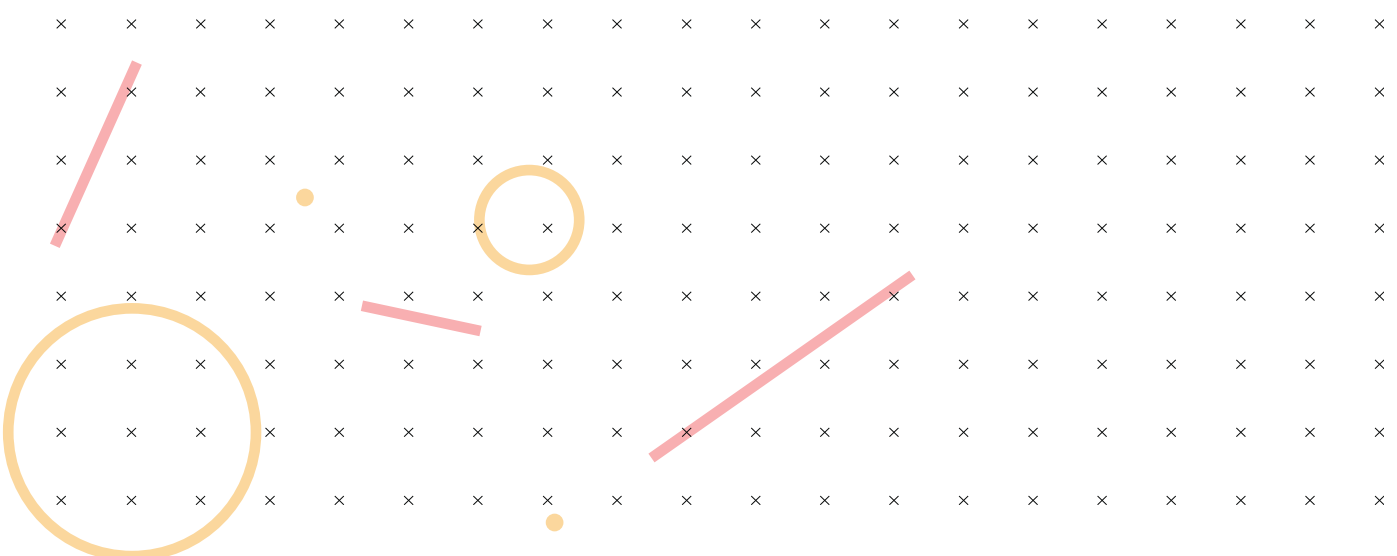
Auch ein gutes Pferd muss trainiert werden

Schon mit einigen wenigen Einstellungen, kann ein Browser um einiges datenschutzfreundlicher werden. Bei einem Browser wie *Chrome* ist es unbedingt notwendig, diese Möglichkeit zu nutzen, da die Standardeinstellungen seinem Geschäftsmodell entsprechend maximal datenhungrig sind. *Firefox* hingegen bietet seinen Nutzer:innen bereits in den Standardeinstellungen einen guten Schutz der Privatsphäre. Da die Möglichkeiten der Datenschutzeinstellungen mit den Browsern zusammen variieren, lässt sich keine Pauschalempfehlung für datenschutzfreundliche Einstellungen abgeben. Trotzdem gibt es einige Punkte, die man bei den Datenschutzeinstellungen aller Browser beachten sollte. Dazu gehören:

- Datenschutzfreundliche Standardsuchmaschine festlegen (z. B. *DuckDuckGo*)
- Passwortspeicherung und andere Auto-Fill-Speicherfunktionen deaktivieren
- Browserdaten regelmäßig löschen
- Führen einer Chronik deaktivieren (wenn möglich, z. B. bei *Firefox*)
- Unnötige Cookies blockieren, insbesondere Drittanbieter-Cookies
- Pop-ups blockieren
- „Do-Not-Track“ Funktion aktivieren

Insgesamt ist es zu empfehlen, bei der Einrichtung des Standardbrowsers einmal alle Sicherheitseinstellungen Stück für Stück durchzugehen. Denn je nach Browser können potentiell auch noch weitere individuelle Schutzmaßnahmen für die Privatsphäre ergriffen werden.

Wenn du bis hierher gelesen und dir vorgenommen hast, deinen Browser mithilfe der richtigen Einstellung gegen den Krieg der Kekse zu rüsten, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen.



In aller Munde

Cookies sind spätestens seit der Datenschutz-Grundverordnung (DSVGO) 2018 durch die Europäische Union in aller Munde. Oder nicht? Das Cookie-An-und-Ablehnen ist eine lästige Tätigkeit, die durch das manipulative Design vieler Cookie-Auswahl-Banner nicht gerade erleichtert wird. Wer in Eile ist, lässt sich daher gerne mal ein ganzes Dutzend Cookies andrehen, die sich mit dem persönlichen Datenschutz nicht besonders gut vertragen. Aber wie kann man Cookies so akzeptieren, dass man seine Daten schützt und die entsprechende Webseite trotzdem problemfrei besuchen kann? Und was sind Cookies überhaupt? Schau dir das folgende Video an, um herauszufinden, wie du Cookies pragmatisch und datenschutzfreundlich akzeptieren kannst:

youtube.com/watch?v=p4Y7l_RyZoM&t=1s

Wenn dir die Wortspiele nicht auf den Keks gegangen sind, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen!

Datenschutz-Tuning

Deinen Browser kannst du mithilfe von kleinen Programmen tunen, sogenannte Plugins. Diese kleinen Helfer kannst du in deinem Browser installieren. Sie unterstützen dich bei allen möglichen Sachen, aber auch bei der digitalen Selbstverteidigung. Hier eine kleine Auswahl an Programmen, die für dich diesbezüglich nützlich sein könnten:

Privacy Badger
Der *Privacy Badger* ist ein Browser-Plugin, welches (auch unsichtbare) Tracker anhand von ihrem Verhalten automatisch erkennt und blockiert, wenn sie ohne deine Zustimmung deine Aktivitäten verfolgen. Das Plugin muss nur im Browser installiert werden und läuft sofort, ohne das weitere individuelle Einstellungen vorgenommen werden müssen. Der *Privacy Badger* bietet somit eine solide Datenschutzgrundlage fürs Surfen, auch für Menschen, die sich mit den technischen Details nicht auseinandersetzen wollen oder können. Gut zu wissen: Der *Privacy Badge*r ist von der *Electronic Frontier Foundation (EFF)* entwickelt worden, einer gemeinnützigen Organisation, die sich für zivilgesellschaftliche digitale Freiheiten einsetzt und keine ökonomischen Interessen verfolgt.

HTTPS Everywhere
Die Abkürzung HTTPS steht für „Hypertext Transfer Protocol Secure", das heißt: „Sicheres Hypertext-Übertragungsprotokoll". Durch diese Übertragungsprotokoll kommunizieren Webbrowser und Webserver miteinander. Im Gegensatz zum HTTP (das gleiche wie HTTPS nur ohne ‚Secure') verschlüsselt HTTPS diese Kommunikation. Wer durch HTTPS kommuniziert, ist also deutlich besser geschützt. Welches Übertragungsprotokoll benutzt wird, legt der:die Betreiber:in der jeweiligen Webseite fest. Das Browser Plugin *HTTPS Everywhere* ermöglicht es Nutzer:innen jedoch, die Kommunikation mit allen dafür geeigneten Webseiten durch HTTPS zu verschlüsseln, auch wenn diese das nicht von sich aus anbieten.

Click & Clean
Auch die besten Datenschutzeinstellungen halten einen Browser im Regelfall nicht davon ab, Informationen über seine Nutzer:innen zu sammeln. Mit dem Browser-Plugin *Click & Clean* können die Browser *Google Chrome* und *Firefox* einer Art Grundreinigung unterzogen werden. Nutzer:innen können dabei individuell einstellen, was genau zu welchem Zeitpunkt und unter welchen Bedingungen gelöscht werden soll. So können durch *Click & Clean* z. B. alle Browserdaten automatisch gelöscht werden, sobald der Browser geschlossen wird.

Wenn Du bis hierher gelesen hast und eventuell schon deine Daten getunet hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen.

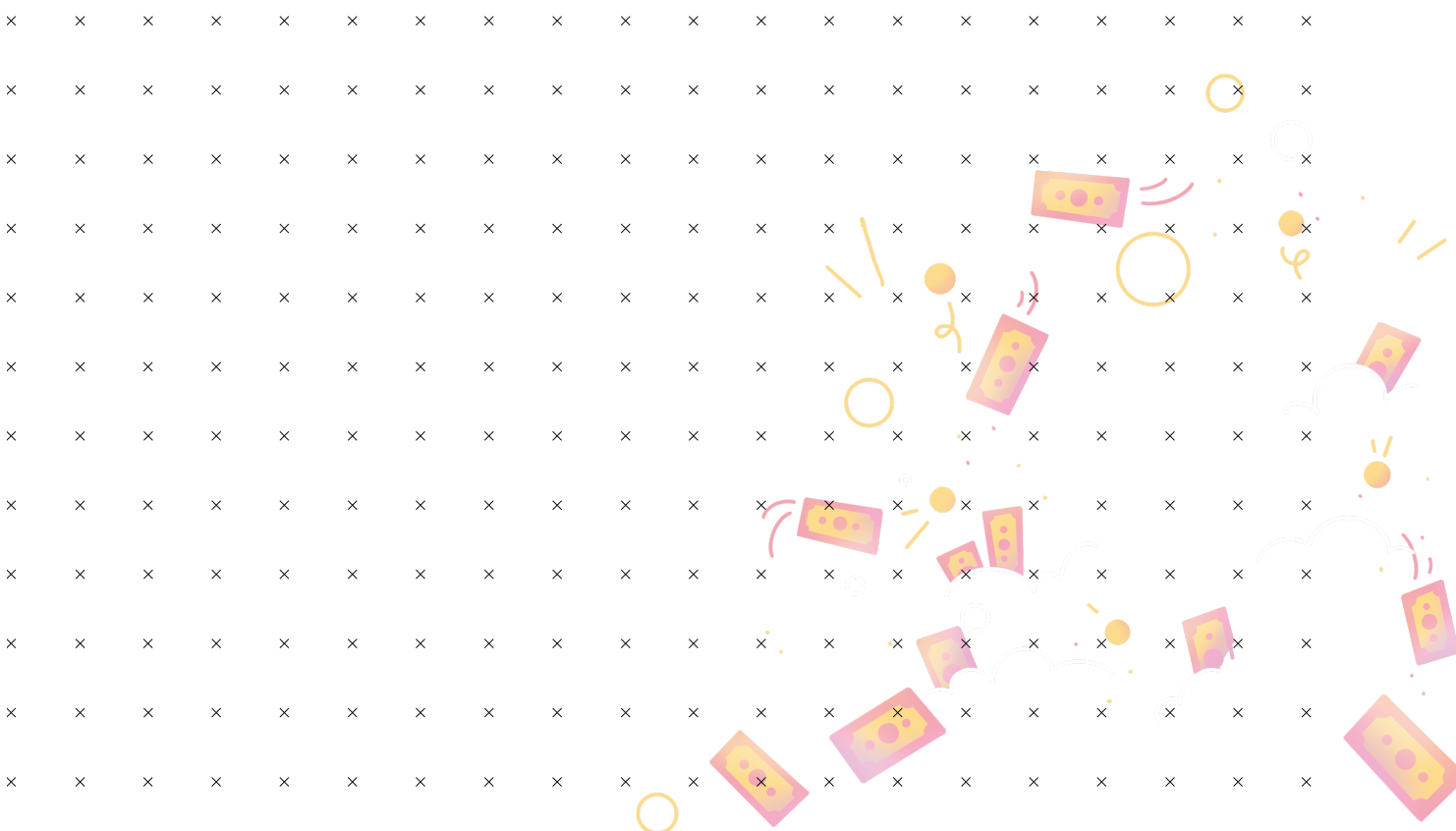
Alternativlos?

Häufig sind datenschutzfreundliche Alternativen zu bekannten digitalen Tools vorhanden, aber schlicht nicht bekannt. Es lohnt sich deshalb, einfach kurz zu recherchieren, welche datenschutzfreundlichen Alternativen es gibt, bevor man unbedacht wieder auf die datenhungrigeren Tools zurückgreift. Hier ist eine kleine unvollständige Liste solcher alternativen Optionen, die du in den meisten Fällen sogar kostenlos nutzen kannst:

Aus Sicht des Datenschutzes ist...

... *DuckDuckGo* besser als *Google*
... *nuudel* besser als *Doodle*
... *Vimeo* besser als *YouTube*
... *Signal* besser als *WhatsApp*
... *Posteo* besser als *GMX*-Mail
... *OpenStreetMap* besser als *Google Maps*
... *Jitsi* besser als *Zoom*
... *Mozilla Firefox* besser als *Google Chrome*
... *CryptPad* besser als *Google Docs*

Wenn du dir vorgenommen hast, deinen nächsten Termin zu nuudeln anstatt zu doodeln, kannst du dich mit einem Seepferdchen-Punkt belohnen!



Ich gelobe Besserung!

Am 28. Januar jedes Jahres ist der Europäische Datenschutztag. Der Tag wurde in Erinnerung an den 28. Januar 1981 gewählt, an dem die Europäische Datenschutzkonvention unterzeichnet wurde, und soll die Bürger:innen Europas für den Datenschutz sensibilisieren.

Nimm dir kurz Zeit, um zu überlegen, welche drei Datenschutzkniffe aus der Stationenarbeit du bis zu diesem Datum in deinem Alltag integrieren möchtest. Schreibe anschließend mithilfe von mailnudge.de eine Email an dich selbst, welche du auf den 28. Januar im nächsten Jahr datierst: Wünsche dir in dieser Email einen frohen Datenschutztag und erinnere dich selbst daran, was du bist dahin für den Schutz deiner personenbezogener Daten und deiner Privatsphäre getan haben möchtest.