

DANN HABEN DIE HALT MEINE DATEN. NA UND?

EIN BUCH FÜR ALLE, DIE NICHTS ZU VERBERGEN
HABEN

KLAUDIA ZOTZMANN-KOCH

EDITION SILBENREICH

Vierte, überarbeitete und erweiterte Auflage

Copyright ©
Klaudia Zottmann-Koch
2019-22

Coverfoto & -design: Klaudia Zottmann-Koch



DANKE

Liebe Leser:innen,

herzlichen Dank, dass Ihr dieses Buch erstanden habt. Ich freue mich sehr darüber. Jeder Buchkauf ist nicht nur ein Stück meines Einkommens als selbständige Autorin, sondern motiviert vor allem ungemein. Ich danke Euch für diese doppelte Unterstützung.

Viel Spaß beim Lesen und bei der Umsetzung!

Eure Klaudia

INHALT

<i>Infos</i>	vii
<i>Vorwort zur vierten Auflage</i>	ix
<i>Geleitwort</i>	xiii
<i>Wie ich selbst von einer »normalen Anwenderin« zur »zertifizierten Datenschutzexpertin« wurde</i>	xvii
TEIL I	
HINTERGRÜNDE	
1. Zitronenfalter falten keine Zitronen	3
2. Auf der Datenautobahn	13
3. Das Internet hinter den Displays	21
4. Tracking – Die tägliche Verfolgungsjagd	44
5. Algorithmen & »KI«	80
6. Social Media	90
7. Web 3.0, NFT & Blockchain	96
8. Gesellschaftliches	107
9. Fragen, Fragen, Fragen	116
10. In trockenen Büchern	119
TEIL II	
DAS KÖNNNT IHR TUN	
11. Das Offline	129
12. Was jeder:r in unter 30 Minuten tun kann	134
13. Social Media Alternativen	189
14. Fortgeschritten	195
15. Etwas weiter fortgeschritten	205
16. Nachwort	208
17. Linkssammlung	214
18. Leseempfehlungen	220
<i>Dank an die Mitwirkenden</i>	223
<i>Eine große Bitte an Euch</i>	225
<i>Neues von Klaudia Zotzmann-Koch</i>	227
<i>Bücher von Klaudia Zotzmann-Koch</i>	229
<i>Vielleicht mögt Ihr auch ...</i>	231

INFOS

Arbeitsblätter

Ab dieser vierten Auflage enthält das Buch Arbeitsblätter für den leichten Einstieg ins Umsetzen.

Für Schulklassen, die die Themen gemeinsam bearbeiten wollen sowie für Menschen, die bereits frühere Ausgaben des Buchs haben, oder diejenigen, die nicht in ein gedrucktes Buch schreiben möchten, gibt es die Arbeitsblätter auch zum Download unter CC-BY-SA 4.0 Lizenz auf meiner Webseite.

<https://www.zotzmann-koch.com/na-und/>



Disclaimer

Dieses Buch ist für Technik-Laien geschrieben, für Menschen, die bislang vielleicht nicht viel mit Datenschutz am Hut hatten. Daher sind die technischen Inhalte stark vereinfacht und schematisiert, um die komplexe Thematik möglichst verständlich zu machen. Die technisch Interessierten mögen es verzeihen.

Außerdem ist die sehr persönliche, eher lapidare Ansprache Absicht, um den teils sehr abstrakten Themen die Distanz zu nehmen.

Die Nennungen von konkreten Browsern, Plugins, Suchmaschinen, Messengern, etc. sind Vorschläge. Es sind Programme, die ich selbst benutze oder kenne. Ich bekomme kein Geld dafür, dass ich sie hier nenne. Wenn vorhanden, stelle ich Euch mehrere Alternativen zu einem Service vor, sodass Ihr Eure eigene Entscheidung treffen könnt.

An einigen Stellen gibt es Links, die auf Angebote Dritter verweisen, auf die ich keinen Einfluss habe und ich somit für deren Inhalte etc. keine Gewähr übernehme.

Alle in diesem Buch verwendeten Marken- und Produktnamen sind Eigentum der jeweiligen Unternehmen. Die Inhalte wurden mit großer Sorgfalt und Genauigkeit erstellt, für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte übernehme ich jedoch keine Gewähr. Sollte Euch ein Fehler auffallen, freue ich mich sehr über eine Nachricht an na-und@zotzmann-koch.com.

Die Quellenangaben stellen nur eine Auswahl von zumeist einer Fülle an Informationen dar. Ich lade Euch ein, selbst weiter zu recherchieren und Euch zu informieren. Sollte Euch dabei auffallen, dass es noch viel bessere Quellen gibt, oder ich einen Sachverhalt falsch oder nicht scharf genug dargestellt habe, freue ich mich ebenfalls über eine Nachricht an na-und@zotzmann-koch.com.

Auf der Buch-Detailseite zotzmann-koch.com/book/na-und gibt es eine Unterseite mit Updates, weiteren Links und Quellen.

VORWORT ZUR VIERTEN AUFLAGE

Facebook heißt jetzt Meta (also der Konzern, nicht die Plattform) und Google Analytics ist seit Neuestem illegal. Google Fonts auch. Und diese mehrseitigen Cookiebanner mit vorausgewähltem »berechtigtem Interesse« ebenso. Es passiert ein bisschen was im Bereich Datenschutz und Privatsphäre und ich höre seltener »ich habe ja nichts zu verbergen«, aber dafür öfter »es ist mir nicht egal, aber ich kann ja nichts machen«. Das stimmt nur zum Teil. Wir können eine Menge tun, um unseren eigenen kleinen Vorgarten sauber zu halten und anderen Menschen davon erzählen, dass sie in ihrem Vorgarten anfangen. Denn Nichts tun ist nur eine schlechte Option, nachdem wir nicht nur für unsere eigenen Daten, sondern auch für die all derer verantwortlich sind, von denen wir Kontaktdaten, Fotos, Videos oder sonstige persönliche Informationen bei uns auf unseren Geräten, in Cloud-Speichern oder auf Social Media gepostet haben.

Ich tue mich schwer damit, einen genauen Punkt auszumachen, an dem die Themen Privatsphäre und Datenschutz wirklich Fahrt aufnahmen. Es werden jedenfalls die Zeitungsausschnitte mehr, die ich von meiner Familie per Messenger geschickt bekomme. In kleinen Lokalzeitschriften wie auch überregionalen Blättern wird zunehmend über Google, Facebook, WhatsApp und wie sie alle heißen aufgeklärt und berichtet. Kritisch durchaus und mit Möglichkeiten, den jeweiligen Unternehmen ein Schnippchen zu schlagen. Wir sind auf einem guten Weg.

Für die letzte Neuauflage war der Fall des PrivacyShields ein ausschlaggebendes Ereignis. Für diese hier sind es vielmehr einzelne, vermeintlich klei-

nere Ereignisse, Gerichtsentscheidungen, und Entscheidungen von Datenschutzbehörden, die sich in kurzer Zeit zusammenlängerten.

Auch wenn ich mir den bisherigen Verlauf des noch sehr jungen Jahres 2022 ansehe: Drei wichtige Entscheidungen sind bereits gefallen: Noch im Dezember 2021 entschied die Datenschutzbehörde in Österreich, dass Google Analytics, also Googles weiterverbreitetes Webseiten-Analysetool, rechtswidrig ist.¹ Keine vier Wochen später gab es eine Entscheidung des Landesgerichts München, dass Google Fonts, also Schriftarten, die von Google Servern an Webseiten ausgespielt werden, rechtswidrig sind.² Anfang Februar erklärt die belgische Datenschutzbehörde den technischen Standard hinter Einwilligungen zu Werbezwecken für rechtswidrig.³ Und nur einen Tag später entschied das irische ICCL, dass die Cookie-Banner nach iab-Standard rechtswidrig sind.⁴ Iab steht für Interactive Advertising Bureau und deren Cookie-banner-Design-Standard ist das mit den mehreren Unterseiten und verstecktem und auch noch vorangehaktem »berechtigtem Interesse«.

Das war der Tag, an dem ich beschloss, diese Neuauflage endlich anzugehen, ehe ich nicht mehr nachkomme mit dem Überarbeiten. Bitte schaut auf meiner Webseite nach möglichen weiteren Änderungen.

All diese Entscheidungen passieren natürlich nicht aus heiterem Himmel oder weil »die da oben« sich darum kümmern, weil's auf ihrer To-Do-Liste steht. Das alles passiert, weil viele Menschen wie Ihr und ich uns mit den Themen auseinandersetzen, recherchieren, darüber reden. Zum Beispiel mit der Nachbarin. Und die trifft im Kindergarten beim Abholen den Vater eines anderen Kindes. Und der ist im Landtag. Und so geht die Sache weiter. Ein gutes Beispiel für eine »Grassroots-Bewegung«; eine Bewegung, in der Themen von unten nach oben sickern.

Und etwas mehr als zwei Jahre nach der Veröffentlichung der ersten Auflage sitze ich hier und aktualisiere erneut ein Sachbuch über Datenschutz, bei dem sich weitere Teilbereiche geändert haben – zum Besseren. Dank Euch und all den Menschen, die über die Themen lesen, weiter recherchieren, darüber reden, bloggen, podcasten und auf Social Media posten. Und die hinterfragen, wenn bestimmte Software von US-Konzernen z. B. im Bildungsbereich eingesetzt werden soll. Die nicht alles hinnehmen, was Typen in Anzügen für viel Geld an ahnungslose Menschen in Zugzwang verscherbeln. Gut so. So funktioniert eine aufgeklärte Gesellschaft und so funktioniert Demokratie.

Ja, manche Debatte ist mühsam und macht keinen Spaß. Wer weiß das besser als ich, die (auch noch als Frau) versucht, für das Thema Datenschutz eine Lanze zu brechen? Aber es ist gut, wenn sie geführt werden. Nichts ist

tödlicher für eine Debatte als »toxische Positivität« – das Wort habe ich 2020 gelernt. Es bezeichnet den Zustand, wenn eine Stimmung oder Gruppenkultur vorherrscht, in der nichts Aufreibendes gesagt werden darf. Wo jeder Konflikt und jede Diskussion über Missstände ums Verrecken vermieden wird. Wo Diskussion und gemeinsame Konsensfindung in Anbetracht aller Fakten unerwünscht sind. Toxische Positivität bringt uns gesellschaftlich nicht weiter, weil Missstände nie aufgezeigt werden dürfen. Übrigens ist »Trollen« die zweite Art, mit der wir kein Stück weiterkommen; also das opportunistische Auf-Alles-Draufschlagen, bis die Parteien der Diskussion so gespalten sind, dass keine Kommunikation mehr möglich ist. Dazu gehört auch »Derailing«, also das Ablenken vom Thema und ebenso »Whataboutism«, also ebenfalls Ablenken, aber mit der Frage »aber was ist mit XY, die auch ein Problem haben?!«.

2022 hänge ich an diese Liste noch an, dass ich zunehmend Menschen begegne bin, die lauthals verkünden, dass man ja nirgendwo mehr frei seine Meinung sagen darf, weil man dafür gleich »geächtet würde«, wie es die letzte Person ausdrückte, die dies laut und öffentlich sagte. Der Ironie dürfen wir hier eine Gedenkminute abhalten. All jenen sei gesagt: Wir leben hier – glücklicherweise! – in einer Demokratie, zu der Meinungsfreiheit essentiell dazu gehört. Andere Menschen auf dieser Welt haben dieses Privileg nicht. Denn Meinungsfreiheit bedeutet, dass wir öffentlich frei unsere Meinung äußern dürfen, solange sie eine Meinungsäußerung und keine rechtswidrige Äußerung (z. B. Nazi-Propaganda oder Aufruf zu Straftaten) ist, und wir für diese Meinungsäußerung nicht belangt werden. Meinungsfreiheit bedeutet nicht, dass ich eine Meinung habe und alle anderen die Freiheit, diese eine, meine Meinung teilen zu müssen. Alle anderen dürfen ihre eigene Meinung haben und frei äußern und wir alle müssen es aushalten, dass diese Meinungen auch unterschiedlich sein können. »Agree to disagree« nennen die Briten das. Und von gespaltener Meinung können die wohl ein Liedchen singen.

Es ist großartig, dass Ihr Euch hier mit diesem sich langsam wandelnden, und immer noch für viele aufreibenden Thema beschäftigt. Wir brauchen als Gesellschaft Menschen, die sich mit den kritischen Themen befassen. Die auf Wissenschaftler:innen und in dem Fall Datenschutzexpert:innen und auch IT-Forensiker:innen vertrauen. Die genau hinschauen, was tatsächlich in einer Software passiert, welche Daten erhoben und irgendwohin übertragen werden, wo sie nichts zu suchen haben. Und die dann die Frage stellen: cui bono? Wo fließt hier das Geld?

Danke, dass Ihr ein Teil davon seid. Und danke, dass Ihr Euch mit den Themen auseinandersetzt, die mir – wie einer immer größer werdenden Menge an Menschen – sehr am Herzen liegen. Viel Spaß beim Lesen und beim Entdecken der vielfältigen Möglichkeiten, es anders zu machen.

Klaudia Zottmann-Koch

1. <https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal>
2. <https://rewis.io/urteile/urteil/lhm-20-01-2022-3-o-1749320/>
3. <https://netzpolitik.org/2022/datenschutzgrundverordnung-wichtiger-baustein-fuer-cookie-banner-ist-illegal/>
4. <https://www.iccl.ie/news/gdpr-enforcer-rules-that-iab-europes-consent-popups-are-unlawful/>

GELEITWORT

von Katharina Larisch & Volker Wittpahl

Dass es unter der schönen bunten Oberflächen unserer digitalen Welt brodelt und im verborgenen quirlig werkelt, bekommt ein jeder von uns mit, wenn eine irritierend treffende Werbeanzeige oder Kaufempfehlung sich in unserem Browser öffnet und man sich leicht beklemmt die Frage stellt: »Woher wissen die, obwohl ich doch ...?«

Obwohl ich doch, ... nichts gemacht habe? Ja, genau deshalb! Weil ich nichts gemacht habe: Weil ich die AGBs nicht gelesen habe, weil ich die Firmware nicht upgedatet habe, weil ich nicht nachgedacht habe, bevor ich die Google-Suche genutzt oder bei Facebook etwas gepostet habe!

Wo ist das Problem? Ich habe doch nichts zu verbergen. Das mag sein, aber ich habe definitiv etwas zu verlieren. Was wir zu verlieren haben verbirgt sich hinter dem eher unattraktiven und zum Teil mit negativen Assoziationen versehenen Begriff »Datenschutz«:

Datenschutz – dieses Wort löst Widerwillen aus.

Datenschutz – das ist ein administratives Monster, welches mein Leben erschwert.

Datenschutz – das ist das Totschlagargument, um ungeliebte Prozesse abzuwürgen.

Dabei ist Datenschutz unser Grundrecht, welches uns gegen den Datenhunger von Konzernen und Organisationen schützt. Es verhindert Profiling und damit Diskriminierung.

Klaudia hat uns ein Jahr lang als Coach begleitet, um uns für den Umgang mit Daten in der digitalen Welt zu sensibilisieren und Wege aufzuzeigen, wie man sich als technischer Laie wappnen kann. Das vorliegende Buch liest sich für uns wie eine Zusammenfassung ihrer Coaching-Sitzungen.

In den Sitzungen hat sie uns aufgezeigt wie perfide und jeglichen Datenschutz missachtend heute von vielen Konzernen Nutzerdaten abgegriffen werden, um daraus Milliardengewinne zu generieren. Auch die Datenschutzgrundverordnung, kurz DSGVO, wird dabei häufig missachtet oder die vermeintlichen Bestimmungen werden so umständlich beschrieben, dass jeder einfach zustimmt, weil man die Tragweite der Zustimmung nicht erfasst.

Dank Klaudia sind wir in der Lage besser zu verstehen, was mit unseren Daten passiert und so informierte Entscheidungen zum Umgang mit unseren Daten zu treffen. Jedem, den wir treffen, erzählen wir davon. Ganz häufig kommt dann die »Ich habe nichts zu verbergen«-Diskussion und wir versuchen aufzuklären, welche Verantwortung jeder einzelne für sich und die Gemeinschaft hat.



Die überarbeitete 2. Auflage ist da – was hat sich geändert? Bei vielen Menschen nicht sehr viel und schon gar nicht unter Corona-Bedingungen. Als Emotet wütete, waren wir froh, dass auf all unseren Privatrechnern nur noch Linux läuft und wir statt Microsoft Office LibreOffice nutzen. Als bekannt wurde, dass im Rahmen vom Solarwind Virus auch Microsoft OneDrive korrumptiert sein könnte, waren wir froh, dass unsere Daten schon seit zwei Jahren auf einer privat gehosteten Cloud liegen. Um Datenschutz muss man sich selbst kümmern und das ist so mühsam wie den inneren Schweinehund zu überwinden, um sich gesund zu ernähren oder sich ausreichend zu bewegen. Bei den letzteren beiden siegt die Ratio über den Schweinehund und beim Umgang mit digitalen Lösungen inzwischen auch.

Bei einigen Anwendungen ist die freie Open-Source-Welt komplizierter oder weniger komfortabel, aber sie funktioniert. Manchmal fordert sie auch Geduld und die Auseinandersetzung mit ihr, da nicht für jedes gemeinnützige Open-Source-Softwareprojekt genug Menschen verfügbar sind, die tolle

Bedienungsanleitungen schreiben. Aber das ist wie Sport, da musst man durch, nicht um dem Herzinfarkt zu entgehen sondern dem Profiling der Datenkraken.



Nun liegt die überarbeitete 4. Auflage vor und die Welt hat sich weitergedreht. Zwei Jahre Pandemie zeigen, wie anfällig unsere globalen Wirtschafts- und Gesundheitssysteme sind. Zwei Jahre haben Menschen noch intensiver Internetdienste und digitale Geräte genutzt. Nicht nur das Coronavirus schaffte den Sprung zur Pandemie, auch die digitale Schädlinge haben sich rasend vermehrt: Eine amerikanische Pipeline wurde lahm gelegt, die Rechner des Landkreises Bitterfeld verschlüsselt und die Technische Universität Berlin konnte über Monate nicht mehr digital arbeiten. Immer mehr „Einzelfälle“ zeigen, wie verwundbar unsere digitale Infrastruktur ist.

Währenddessen saßen viele von uns zu Hause bei Streaming-Angeboten von Netflix und noch mehr Lieferungen von Amazon. Manche konnten und durften von zu Hause arbeiten, so dass Videokonferenzen nicht mehr Privileg sondern das neue Normal in allen Lebenslagen sind. Aber nicht nur wir saßen zu Hause, sondern auch die Hacker. Sie haben ihre Methoden optimiert. Ebenso entwickelten die global agierenden Datenhändler ihre Werkzeuge und Angebote weiter und freuen sich über die täglich mehr werdenden Datenn Mengen.

Wenn ich nichts zu verbergen habe, warum gibt es dann noch Bankgeheimnis, Wahlgeheimnis, ärztliche Schweigepflicht und Briefgeheimnis?

Wenn uns diese Errungenschaften in der physischen Welt wichtig sind, so müssen wir sie auch in der digitalen Welt verteidigen. Viele Menschen ist dies im Umgang mit digitalen Diensten aber nicht bewusst. Sonst hätten sie den ein oder anderen vermeintlich freien Dienst nicht einfach genutzt und ihn dabei mit wertvollen persönlichen Daten versorgt.

Mit der 4. Auflage ist nun dem digitalen Laien die Möglichkeit gegeben, sich den neuen Bedrohungen bewusst zu werden und sich entsprechend abzusichern.

– Katharina Larisch & Volker Wittpahl

WIE ICH SELBST VON EINER »NORMALEN ANWENDERIN« ZUR »ZERTIFIZIERTEN DATENSCHUTZEXPERTIN« WURDE

Diesen Teil könnt Ihr gerne überspringen. Die spannenden Teile, warum Ihr Euch mit Privatsphäre beschäftigen solltet und was alles geht, kommen ab Kapitel 1.

Ihr müsst nicht irgendwas mit IT oder Technik studiert oder eine mehrjährige Ausbildung in dem Bereich gemacht haben, um die Themen »Privatsphäre« und »Datenschutz« zu verstehen. Es reicht, Euch damit zu beschäftigen und ggf. auch nicht locker zu lassen, wenn Euch eine Frage umtreibt.

Es ist gar nicht so lange her, da war ich eine normale Internetnutzerin. Ich hatte seit 2007 ein Facebook-Konto, nutzte Gmail und web.de und davor auch Myspace und StudiVZ. Ich arbeitete mit Google Docs und nutzte Google Maps, wenn ich mich irgendwo nicht auskannte. Ich »skypete« regelmäßig mit meiner Mutter und meiner Oma, hatte Evernote und Dropbox auf allen meinen Geräten und insgesamt wenig Ahnung, wie das Internet funktioniert, wie Werbetechnologien arbeiten und all die anderen Sachen, von denen später noch die Rede sein wird. Ich hatte sogar mal Kundenkarten.

Dann wechselte ich von der Uni zu einer Vollzeitstelle als Projektmanagerin in der Webentwicklung und lernte, wie das Internet funktioniert, wie man große Webseiten, Onlinespiele und Apps baut und auch, wie man Tracking, also Besucherzählung und Analyse von Nutzer:innenverhalten, einbaut und nutzt. Zu dem Zeitpunkt war es mein Job, Kundenprojekte zu begleiten und umzusetzen und noch immer war ich mit Facebook-Veranstaltungen und -Fotoalben und allem oben genannten fleißig dabei.

Und dann gab es mehrere Ereignisse in meinem Leben, nach denen ich das vage Gefühl hatte, dass mir »Die« zu nahe auf die Pelle rückten. Personalisierte Werbung über mehrere Geräte hinweg war mir unangenehm. Bei einem Skiurlaub wusste mein Exmann genau, wo ich gefahren war, bevor ich ihm davon erzählte, weil die Familienfreigabe im Telefon ihm live anzeigte, wo sich mein Telefon – und damit auch ich – befand. Auch abseits dessen empfand ich zielgerichtete Angebote und Informationen zunehmend als übergriffig. Dabei ging es gar nicht darum, dass ich »etwas zu verbergen« hatte. Ich erzählte meinem Exmann ja auch selbst, dass ich todesmutig mit dem Skikurs die Anfängerstrecken hinunter gerast war (mit vermutlich 10 km/h). Ich fand es nur irritierend, dass er es bereits wusste.

Genauso wie viele andere ging ich damals der Illusion auf den Leim, dass »etwas zu verbergen haben« gleichbedeutend sei mit »etwas verbrochen zu haben«.

Ich jubelte, als *Anonymous* Websites des IS übernahm und mit Werbung für Potenzmittel bespielte. Ich feuerte die Jungs und Mädels von *Anonymous* an: »Go, guys, go!« Und ich beschloss, mich näher mit diesem Thema »Internetsicherheit« zu beschäftigen.

Später im selben Jahr besuchte ich meine erste »Cryptoparty«, einen jener Abende, die es in quasi jeder größeren Stadt gibt, an denen man von fachkundigen Menschen lernen kann, wie man die eigene Privatsphäre schützen kann; beispielsweise wie man eMails verschlüsselt, wie man sein Telefon sicherer macht etc. Ich wollte damals wissen, wie das mit dieser Verschlüsselung grundsätzlich funktioniert. Nicht wegen meines Exmanns, sondern weil ich schrecklich neugierig bin. Noch ein bisschen später zog ich dann bei ihm aus und wohnte zehn Wochen bei einem Kumpel auf der Couch, bis ich eine eigene Bleibe hatte. Während dieser Zeit war ich dann öfter im Wiener Hackspace, dem *Metalab*, weil ich dort mehr »Privatsphäre« hatte, als auf der fremden Couch. Ich lernte nicht nur, wie Verschlüsselung funktioniert und welche Messenger sinnvoller sind als andere und warum, ich lernte auch eine Menge Leute kennen, die im Bereich Datenschutz und IT-Sicherheit wissen, was sie tun.

Im selben Jahr fuhr ich sehr spontan nach Hamburg zum jährlichen Kongress des CCC, des *Chaos Computer Clubs*. Ich war überwältigt. Neben einem ausufernden Maß an buntem Blinken und vielen Spaß-Projekten wie beispielsweise einem Fernschreiber, dem man via Internet Nachrichten schicken konnte, die dann auf Lochstreifen ausgegeben wurden, gab es ein

Vortragsprogramm, das sich gewaschen hatte. Nahezu alles wurde von den Teilnehmer:innen selbst angeboten. Keine bezahlten Vortragenden und schon gar keine »Keynotespeaker«, sondern alles Leute, die in ihren Dayjobs tagtäglich mit dem Zeug arbeiteten, über das sie sprachen. Die Vorträge hatten insgesamt ein derart hohes Niveau, das ich an der Uni nur selten erlebt habe. Bis heute: Hut ab.

Nach diesem Kongress wurde in Wien die lokale CCC-Niederlassung regegründet, die die letzten zehn Jahre eingeschlafen gewesen war. Gleich zu Beginn der Vereinstätigkeit wurden zwei große Projekte gestartet: »Chaos macht Schule« wurde von Deutschland nach Wien geholt. Das bedeutet, dass Menschen in ihrer Freizeit unbezahlt in Schulen gehen und dort Workshops zu Internetsicherheit und Medienkompetenz für Schüler:innen, Lehrende und Eltern abhalten. Viele von ihnen nehmen sich dafür extra einen halben Tag oder auch länger frei, um ehrenamtlich das zu kompensieren, was andere für viel Steuergeld in ihrer Arbeitszeit versäumen. Das andere Projekt, das im selben Jahr startete, ist die »PrivacyWeek«, die seither jährlich stattfindet, 2020 und 2021 aufgrund der Gegebenheiten komplett online. Die Privacy-Week ist eine ganze Woche voller Workshops, Vorträge, Kunstprojekte, Filmvorführungen, Diskussionsrunden und Austausch. Zielgruppe: jede:r, den:die die Themen Privatsphäre, Medienkompetenz, Internetsicherheit und Demokratie interessieren – weil wir unser Wissen und unsere Erfahrungen in die Gesellschaft tragen wollen. Ich bin sehr glücklich, dieses Projekt bis heute mit betreuen und gestalten zu dürfen.

Im Frühjahr 2016, wenige Wochen nach meinem ersten Congress, hatte ich aufgehört, Facebook zu nutzen. Ebenso Google Maps, die Google Suche, WhatsApp, Gmail, web.de, GMX und einiges andere, was mir nicht einmal mehr einfällt. Ich hatte noch Twitter und die eMail-Adresse, die mit dem Webspace meiner Domain gekommen war. Außerdem noch Skype für das sonntägliche Video-Telefonat mit meiner Familie. In meiner Erinnerung habe ich nicht einmal gemerkt, wie ich mich langsam aber sicher von allem anderen verabschiedet hatte.

Ich begann, Vorträge darüber zu halten, welche Dienste datensparsamer sind als andere. Ich erzählte bei Autor:innen-Treffen davon, was Hacker:innen sind und was alles nicht. Und dass niemand, der:die sich mit Internetsicherheit auskennt, jemals »Cyber« sagt, ohne es ironisch zu meinen. (Weil das nämlich von »Kybernetik« kommt und absolut nichts mit dem zu tun hat, wofür es im Marketing und in den Medien verwendet wird.)

Ich lernte im nächsten Dayjob – wieder Projektmanagement Webentwicklung –, wie große Trackinganbieter wie Adobe, IBM und Oracle arbeiten und wie deren Verträge aussehen. Allerdings machte ich wenig Projektmanagement, weil es dafür noch eine eigene Abteilung gab. Stattdessen sollte ich mich 14 Monate lang um Google Werbebanner kümmern. Ich erzählte meinem Arbeitgeber im Wochentakt, dass ich das nicht machen will und warum und kündigte schließlich, als ich noch mehr Werbebanner auf meinen Tisch bekommen sollte.

Stattdessen machte ich die Ausbildung zur Datenschutzbeauftragten. Ich hatte mittlerweile genug gelernt, dass ich mich mit dem Thema wohlfühlte und nach der Prüfung legte ich noch eine weitere bei der österreichischen Wirtschaftskammer zur Datenschutzexpertin ab.

Der 25. Mai 2018, also der Stichtag für die DSGVO, kam und zumindest in Österreich schien damit das Thema gestorben. Schlag Mitternacht war alles ruhig. Fünf Nachzügler-eMails kamen noch am 25. vormittags, ab dann: *Totenstille*. Ab dem Zeitpunkt schaute ich voller Bewunderung nach Deutschland und Frankreich wo Datenschutz tatsächlich durchgesetzt wurde. Von einigen nordischen Ländern ganz zu schweigen. Österreich schaffte es hingegen, drei Wochen vor dem Stichtag die lokale Gesetzgebung so anzupassen, dass »Verwarnen statt Strafen« im Datenschutzgesetz steht. Entsprechend lax ist zuweilen der Umgang mit Datenschutz und gerade mal das Minimum wird in vielen Firmen umgesetzt. Im November 2019 wurde von der Datenschutzbehörde mit der 18-Millionen-Euro-Strafe gegen die österreichische Post erstmals ein ernstzunehmendes Bußgeld gegen ein österreichisches Unternehmen verhängt; dafür, dass sie die politische Einstellung der in Österreich lebenden Menschen erhoben bzw. hochgerechnet und an Werbetreibende verkauft hat.¹ Die Post ging rechtlich gegen die Strafe vor, weil sie darin ihr zentrales Geschäftsmodell gefährdet sah – und kam tatsächlich ohne Strafzahlung davon.² Und das schlug nicht einmal sonderlich hohe Wellen. Wenn ein teilstaatlicher Betrieb sein zentrales Geschäftsmodell im Datenhandel mit sensiblen Daten sieht, sagt das ja auch schon sehr viel aus. Im Übrigen stellen die 18 Millionen ziemlich genau 1 % ihres Jahresumsatzes dar. 4 % wäre die mögliche Maximalstrafe gewesen. Die Datenschutzbehörde scheint also tatsächlich aktiv zu sein – ein Umstand, der in der Bevölkerung und bei den meisten Firmen nur sehr, sehr langsam sickert. Vielleicht trägt ja das Urteil zu Google Analytics³ von Ende Dezember 2021 mehr zur öffentlichen Wahrnehmung bei.

Noch immer gilt: Alle, die es sich leisten können, beauftragen ihre Haus- und Hof-Kanzleien für Datenschutzthemen, ungeachtet dessen, dass Daten-