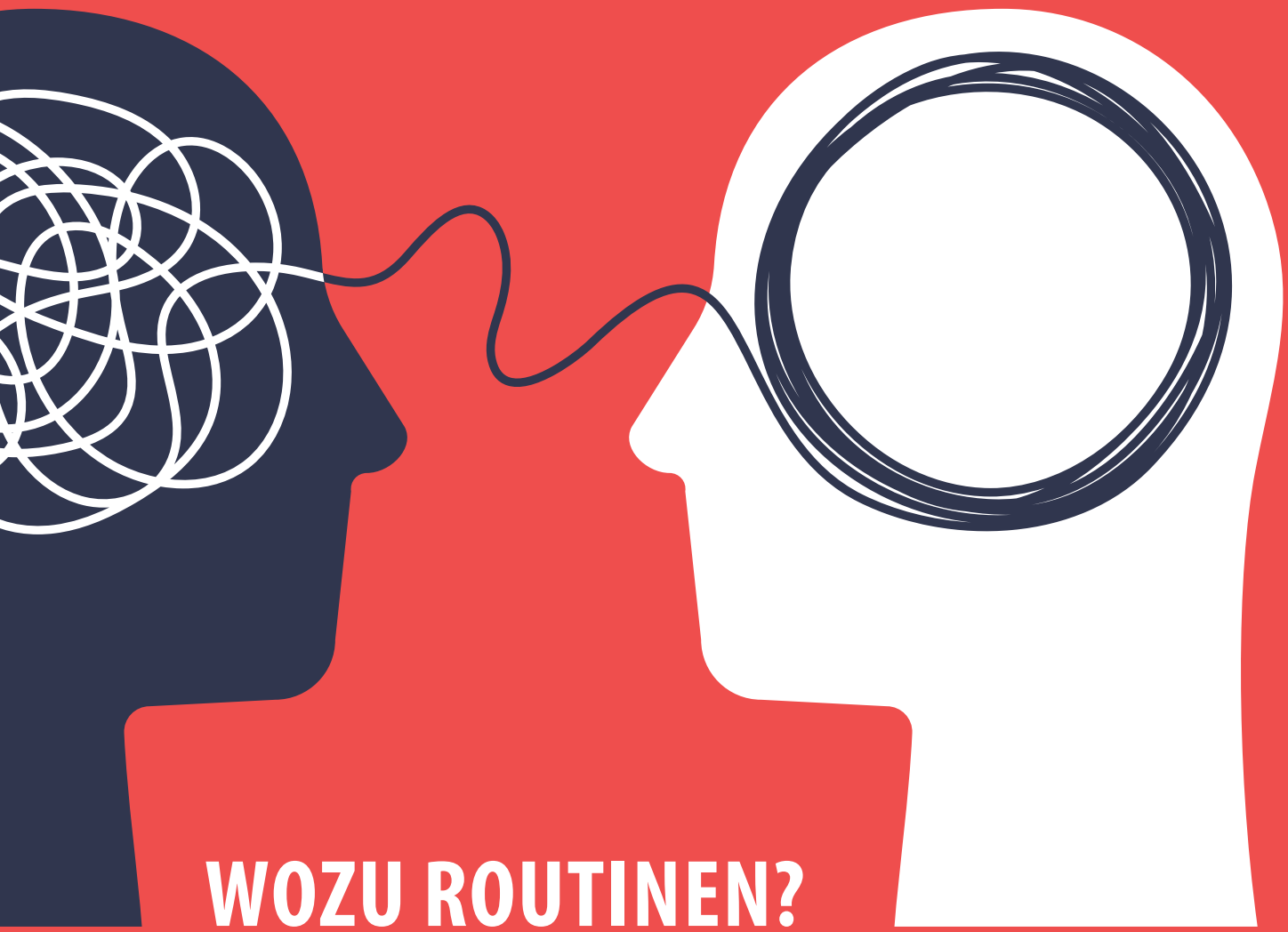
ExperSite

Das Magazin für Digitalisierung, Informationssicherheit und Datenschutz

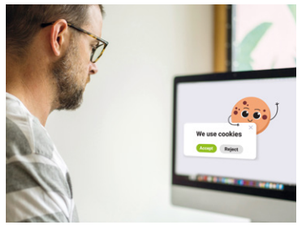
Ausgabe 02 | 2022



WOZU ROUTINEN?

Das ist keine Übung, sondern ein Weckruf!
4

DATATREE Prüfgemeinschaft – Erfolgreich Synergien schaffen 16



Consent-Banner – Wer blickt hier noch durch?
22

ExperSite ist das Magazin der JÄSCHKE GRUPPE für Digitalisierung, Informationssicherheit und Datenschutz

Zur JÄSCHKE GRUPPE gehören die Unternehmen:

JÄSCHKE GRUPPE
GEMEINSAM DIGITALISIERUNG LEBEN

www.dr-jaeschke.ag

Die Sache mit den Vorsätzen oder auch: Nächstes Jahr wird es noch besser!

Hand aufs Herz: Wie sehr mögen Sie Vorsätze fürs neue Jahr? Gehören Sie zu den Enthusiasten, die ab Januar motiviert neue Herausforderungen angehen, oder hören Sie nicht hin, wenn wieder mal der „gesündere Lebensstil“, das „Aufhören mit dem Rauchen“ oder „ab jetzt aber wirklich mehr Sport“ auf der Tagesordnung stehen?

Aussagen über die Etablierung einer Gewohnheit schwanken. Während die einen der Meinung sind, dass sich ein routinierter Ablauf nach acht Tagen einstellt, gehen die anderen von zwei Wochen bis zu drei Monaten aus. Mir persönlich stellt sich eher die Frage, warum immer dieselben Vorsätze auf der Jahres-To-Do-Liste stehen, und mich beschleicht das Gefühl, dass da etwas nicht ganz rund läuft.

Ich habe deshalb einen Vorschlag: Lassen Sie uns doch ganz neue Vorsätze, oder besser „Gewohnheiten” schaffen und schon ab jetzt umsetzen. Zum Beispiel: „Ich betrachte Informationssicherheit als wichtigen Bestandteil meiner Prozesse, um meine Kolleg:innen, mich und das gesamte Unternehmen unangreifbar zu machen.“ Und wenn Sie auch zu denjenigen gehören, die das ohnehin schon so sehen, dann rege ich dazu an, diesen Standpunkt auch anderen zu vermitteln. Denn die Gewohnheit, die Informationssicherheit - insbesondere den Datenschutz - als Bremsklotz der Digitalisierung zu betrachten, sollte Ende 2022 endgültig für alle vom Tisch sein.

Datenschutz darf nicht länger der notorische Bremsklotz sein.

Wenn wir diese Perspektive verinnerlichen und sie nicht jedes Jahr aufs Neue als wiederkehrenden Vorsatz auf die Liste setzen, dann können wir Digitalisierung in 2023 ganz neu und vor allem besser gestalten.

Ich wünsche Ihnen viel Freude beim Lesen dieser Ausgabe und freue mich auf ein erfolgreiches neues Jahr mit Ihnen.

Ihre Nina Kill
(Redaktionsleitung)

Das ist keine Übung, sondern ein Weckruf!

Standards für Digitalisierung, Informationssicherheit und Datenschutz sind vorhanden. Trotzdem scheinen routinierte Abläufe einen schweren Stand zu haben. Der Faktor Mensch spielt einmal mehr eine wesentliche Rolle.

Text: Nina Khan

Die Lage der IT-Sicherheit in Deutschland 2022

Vereinheitlichung, Norm, Richtschnur oder Regel – ganz gleich, wie wir es nennen, klar ist:

Wenn es um Sicherheit geht, genießen Standards einen hohen Stellenwert: Unter 1.500 Flugstunden kann niemand Verkehrspilot werden, einbruchssicher gilt ein Haus mitunter durch DIN-gemäße Nachrüstsysteme für Fenster und Türen und alle, die mit Informationssicherheit in Berührung kommen, kennen den internationalen Standard für die Realisierung eines Informationssicherheitmanagementsystems (ISMS), der in der ISO 27001 verankert ist.

Wenig überraschend und für viele gleichzeitig beruhigend ist, dass Standardisierungen auch vor unserem höchsten Gut - der Gesundheit - nicht Halt machen. „Mindestmenge" lautet hier das Stichwort, unter das die Qualitätssicherung der medizinischen Versorgung bei geplanten Operationen zusammengefasst wird. Seit 2004 wird das Instrument durch den Gemeinsamen Bundesausschuss (G-BA) für die stationäre Versorgung in § 136b Abs.1 Nr. 2 sowie Abs. 3 und 4 SGB V festgelegt.

Entscheiden Routinen über die Qualität?

Was darunter zu verstehen ist, hat der ehemalige Bundesminister für Gesundheit, Jens Spahn, folgendermaßen zusammengefasst: „Wenn in einem Krankenhaus eine komplizierte Operation 20-mal im Jahr durchgeführt wird, kann mir niemand sagen, dass dies in der gleichen Qualität geschieht wie in einem Krankenhaus, das diese Operation 200-mal im Jahr durchführt."

Mindestmenge heißt also: Ein Krankenhaus muss eine gewisse Erfahrung vorweisen, die an der jährlichen Anzahl an planbar durchgeführten Operationen gemessen wird. Die Grenzwerte werden gemeinsam von Kliniken, Ärzten und Krankenkassen festgelegt. Erreicht ein Krankenhaus diese Mindestmenge nicht, kann es die Behandlung nicht vergüten.

Für welche Operationen eine Mindestmenge festgelegt wird, ermittelt der positive Volume-Outcome-Zusammenhang, der einen Zusammenhang zwischen der Behandlungshäufigkeit des Krankenhauses und einer entsprechenden Qualität des Ergebnisses misst. Positiv ist dieser Zusammenhang bei bisher sieben Indikationen, die von verschiedenen Transplantationen über Bauchspeicheldrüsen-OPs bis hin zur Frühgeborenen-Versorgung bis 1.250 Gramm reichen. Die Wirksamkeit von Mindestmengen bei geplanten Operationen wurde bereits in zahlreichen nationalen und internationalen Studien nachgewiesen, zwei davon stammen vom Wissenschaftlichen Institut der AOK (WIdO) und belegen sogar eine deutlich niedrigere Revisionsrate in Kliniken mit hohen Fallzahlen.

Neben der Anzahl der Operationen gibt es weitere Faktoren, die für die Qualitätssteigerung der medizinischen Versorgung ausschlaggebend sind. Hierbei spielen beispielsweise die Ausstattung des Pflegepersonals oder die individuelle Erfahrung des behandelnden Chirurgen eine Rolle.

> Die Gemengelage der Fallzahlen in Krankenhäusern lässt insgesamt das Fazit zu:
> Die Qualität einer medizinischen Versorgung hängt mit großen Anteilen von der Routine des Krankenhauses ab.

Digitalisierung, Informationssicherheit und Datenschutz haben Nachholbedarf bei routinierten Anwendungen

Während Fallzahlen die Qualitätssteigerung bei operativen Eingriffen durch Routine belegen, bestehen für routinierte Abläufe in Digitalisierung, Informationssicherheit und Datenschutz noch Nachholbedarf.

Der Bericht über die Lage der IT-Sicherheit in Deutschland 2022 des Bundesinstituts für Sicherheit in der Informationstechnik (BSI) zeigt besonders plakativ den Stauts Quo: Die Gefährdungslage im Cyber-Raum ist so hoch wie nie. So wurden mehr Schwachstellen und Angriffe auf Perimeter-Systeme, wie beispielsweise Router oder Firewalls identifiziert, die Anzahl der Schadprogramm-Varianten hat um 116,6 Millionen zugenommen, ebenso steigt die Zahl der Opfer von Ransomware-Angriffen mit Schweigegeld-Erpressung.

Letzteres ist vor allem im Zusammenhang mit kritischen Infrastrukturanbietern, insbesondere Krankenhäusern, zu nennen, die ein attraktives Ziel für Hacker darstellen und dadurch vermehrt Ransomware-Angriffen ausgesetzt sind.

Standards, um Personen und Systeme zu schützen, sind vorhanden

Dabei sind auch auf dem Feld der Informationssicherheit Standardisierungen kein Novum: Informationssicherheits-Managementsysteme sorgen für die Einrichtung, Umsetzung und Verbesserung der Informationen in Organisationen und werden nach ISO 27001 weltweit anerkannt.

Weiterhin sind die definierten Ziele „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ fest verankert und sollen einen angemessenen Schutz der Unternehmensinformationen gewährleisten. Die auch unter „CIA-Triade“ (Confidentiality, Integrity und Availability) bekannten Prinzipien schließen im Rahmen der Informationssicherheit auch personenbezogene Daten mit ein, die wiederum dem Datenschutz unterliegen und zudem gesetzlich geschützt sind. In diesem Zusammenhang ist vor allem ein allgemein bekanntes Werk zu nennen: Die Europäische Datenschutzgrundverordnung (DSGVO), die seit 2016 durch die Europäische Union das Verarbeiten von personenbezogenen Daten regelt. Ob es die korrekte Konfiguration eines Consent-Banners auf Websites ist oder der Schutz der Privatsphäre in der Telekommunikation – es werden kontinuierlich Standards geschaffen, um Personen und Systeme zu schützen. Drei Jahre nach ihrer Einführung zeigte eine Studie des Digitalverbands Bitkom allerdings, dass von 500 befragten Unternehmen 97 Prozent Probleme mit der Umsetzung der DSGVO haben. Der Start zum Schutz von Informationen, personenbezogenen Daten und IT-Sicherheit schien mehr als holprig.

Als Gründe hierfür werden häufig Personalmangel, unterschätze Rechte und Pflichten und immer wieder der Mangel an qualifizierten Beschäftigten genannt. Nichtsdestotrotz kann der Schutz von kritischen Infrastrukturen nicht in den Hinterhalt geraten. Mit Einführung des Krankenhauszukunftsgesetz (KHZG) im Jahr 2020 sollen Krankenhäuser durch ein Investitionsprogramm unter anderem in Digitalisierung und IT-Sicherheit unangreifbarer werden.

Statt Datenschutz als Problem zu interpretieren, müssen wir uns an vorhandenen Lösungen bedienen.

ISO 27001, Schutzziele, DSGVO, KHZG – die Rahmenbedingungen sind vorhanden. Dennoch werden Kritiker nicht müde, von „Bremsklötzen“ oder „Innovationsstoppern“ durch Datenschutzrichtlinien zu berichten.

> „Wenn der Faktor Mensch nicht mitbedacht wird, kann kein Gesetz der Welt routinierte Prozesse in der Informationssicherheit durchsetzen”, setzt dem Prof. Dr. Thomas Jäschke, Medizin- und Wirtschaftsinformatiker, entgegen, „am Beispiel der Digitalisierung wird deutlich, dass sie ohne Datenschutz - als Teilbereich der Informationssicherheit - nicht auskommt.”

Anstatt ihn als Problem zu interpretieren, müssen wir Datenschutz leben und beginnen, uns an den durchaus vorhandenen Lösungen zu bedienen. Dass die Gefährdungslage im Cyber-Raum so hoch war wie nie, ist keine Übung, sondern ein Weckruf. Dieser Bedrohungslage gilt es entgegenzuwirken. Durch Audits zur Informationssicherheit, zum Datenschutz und zur IT-Sicherheit, durch Dokumentationssoftwares für Informationssicherheitsmanagementsysteme oder für Datenschutzmanagementsysteme. Vor allem aber dadurch, dass Verantwortliche sensibilisiert und überzeugt davon sind, und auf diese Weise entsprechende Prozesse verinnerlichen und ausführen.

> Nur durch Menschen entstehen Routinen, die den Weg zu einem sicheren System erleichtern und uns zum Ziel führen.

Literatur

www.aok-bv.de/presse/pressemitteilungen/2020/index_23642.html

www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-der-Unternehmen-haben-DS-GVO-groesstenteils-umgesetzt

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=5

Elon Musk schläft auf dem SpaceX-Flur und beginnt ohne Dusche nicht den Tag, Melinda Gates verbringt ihre erste wache Stunde mit Yoga und Michael Phelps hat als Motivationsschub vor jedem Schwimmrennen "'Till I collapse" von Rapper Eminem laufen lassen.

So weit, so routiniert. Da stellt sich schnell die Frage, ob Routinen für einen erfolgreichen Job nicht nur möglich, sondern auch nötig sind.

Erfolg ist kein Zufallsprodukt

EINE BESTANDSAUFNAHME BEI DER DATATREE AG

Nina Khan
interviewte drei Mitarbeitende der DATATREE AG zum Thema Routinen und sprach mit Ihnen über ihr Arbeitsumfeld als Berater:innen in den Bereichen Informationssicherheit und Datenschutz.

Flexibilität mit selbstgewählten Routinen vereint: Andreas Pillen

Mit einem klaren „Ja“ beantwortet das Andreas Pillen. Der Berater für Informationssicherheit ist seit Mai bei der DATATREE AG tätig. Nach einer 25-jährigen Karriere in einem internationalen IT- und Beratungsunternehmen hat sich der gebürtige Mönchengladbacher dazu entschieden, aus dem Vertriebsumfeld in die Beratung zu wechseln.

Nachdem Informationssicherheit schon immer ein latentes Thema in seinem vergangenen Job war, möchte er nun sukzessive sein Know-how in die Kundenberatung integrieren. „Ich empfinde die DATATREE AG als ein spannendes Umfeld, in dem sich viele interessante Menschen aufhalten. Seit meinem Beginn im Mai dieses Jahres bestätigt sich dieser Eindruck täglich aufs Neue”, resümiert Andreas seine bisherige Zeit bei dem Compliance Provider.

Einen routinierten Ablauf in seinem Workflow kann er schnell definieren:

„Ich sehe meinen Beruf als Customer-Relation, in der ich Lösungen für Kund:innen finde. Ein erfolgreiches Ergebnis erhalten wir, indem ich nach einer Ist-Analyse das Ziel mit dem/der Kund:in bespreche, den Weg dorthin festlege und wir diesen anschließend gemeinsam bestreiten. Das ist ein routiniertes Vorgehen und der Grundstein für eine gute Zusammenarbeit.“

Wenn es um allgemeingültige Abläufe im Unternehmen geht, an die sich Mitarbeiter:innen halten, werden Routinen zu Prozessen. Andreas empfindet diese als notwendig: „Prozesse gestalten Strukturen. Das gibt Mitarbeiter:innen Sicherheit in ihrem Handeln. Allerdings ist auch klar: Je größer das Unternehmen ist, desto komplexer werden allgemeingültige Abläufe und desto weniger Einfluss hat der/die Einzelne auf diese.“

Ein Punkt, den Andreas als positiv bei der DATATREE AG wertet: „Wir leben hier eine flache Hierarchie. Wenn ich mit Verantwortlichen über bestimmte Abläufe spreche und Vorschläge mache, ist es sehr wahrscheinlich, dass das auf fruchtbaren Boden fällt. Ich habe also die Möglichkeit, Prozesse aktiv mitzugestalten und Workarounds zu optimieren, wenn es nötig sein sollte. Das schätze ich sehr.“

> *Ich habe die Möglichkeit, Prozesse aktiv mitzugestalten und Workarounds zu optimieren. Das schätze ich sehr.*
>
> Andreas Pillen
> *Berater Informationssicherheit*

Nicht nur, was seinen Umgang mit Kund:innen angeht, hat Andreas Routinen entwickelt: „Beruflich und privat möchte ich zu meinen Commitments stehen. Um das zu erreichen, arbeite ich schon seit Jahren mit To-Do-Listen, die mir einen guten Überblick verschaffen”, erläutert er.

Die DATATREE AG ermöglicht ihm außerdem zeitliche Flexibilität:

So kann er grundsätzlich selbst bestimmen, ob er im Homeoffice arbeitet und wann er seine Pausen einlegt. „Für mich ist diese Freiheit wichtig, um mich und meinen Ablauf zu strukturieren. Natürlich gibt es feste Kundentermine oder interne Meetings, deren Teilnahme vorausgesetzt wird. Grundsätzlich aber kann ich meine Struktur selbst schaffen und dadurch gewährleisten, dass ich am Ende des Arbeitstages das schaffe, was ich mir vorgenommen habe.“

Für Niklas Sommerhage hingegen sind Routinen im Arbeitsalltag bisher nur bedingt umsetzbar. Der 24-Jährige kombiniert seit 2018 sein Informatikstudium mit seiner Tätigkeit bei der DATATREE AG. Eine optimale Voraussetzung hierfür ist sein Studienschwerpunkt im Bereich Informationssicherheit.

Seit April dieses Jahres arbeitet Niklas an seiner Thesis und wechselte von da an seine studentische Aushilfstätigkeit zu einer Vollzeitstelle als Berater für Informationssicherheit und Datenschutz. Für seine Masterarbeit entwickelt er ein IT-Sicherheitskonzept auf akademischer Basis. Bei der Themenfindung wurde er von Magnus Welz unterstützt, der das Team Beratung sowie das IT-und Wissensmanagement der DATATREE AG verantwortet.

> *Bei der DATATREE AG lässt sich ein Studium hervorragend mit einer beruflichen Tätigkeit verbinden.*
>
> Niklas Sommerhage
> *Berater Informationssicherheit*

Studium und Beruf zusammengedacht: *Niklas Sommerhage*

„Natürlich ist es eine Doppelbelastung, noch während des Studierens in den Beruf einzusteigen. Allerdings lässt sich das bei der DATATREE AG durch eine kompetente und gleichzeitig sehr kollegiale Umgebung mit meinen Vorgesetzen und Arbeitskolleg:innen problemlos verbinden", beschreibt Niklas den Spagat zwischen Universität und Beruf. Routinierte Beratertätigkeiten, wie beispielsweise Dienstleister-Audits, sind bisher Ausnahmen auf seiner Agenda. Auf diese Weise kann Niklas den Fokus auf seine Thesis sowie die Entwicklung des IT-Sicherheitkonzepts für die Software MeKidS.support des Förderprojekts MeKidS.best legen.

Es geht auch mal ohne standardisierte Abläufe

Das MeKidS.best-Projekt wird durch den Innovationsfonds des gemeinsamen Bundesausschusses gefördert. Neben der DATATREE AG gibt es 31 weitere Konsortial- und Kooperationspartner:innen. „Da kommen viele Personen zusammen, mit denen ich mich regelmäßig oder unregelmäßig austausche. Die Abstimmung mit internen und externen Ansprechpartner:innen machen einen standardisierten Ablauf kaum möglich – allerdings hat sich das bisher nicht als Problem für mich dargestellt", beschreibt Niklas seinen Berufsalltag, „Im Gegensatz dazu führen interne Meetings im Team dazu, routinierte Prozesse einzuführen und helfen insbesondere Berufseinsteigern wie mir, sich in den Arbeitsalltag einzufinden." Darüber hinaus freut sich Niklas auf verstärkten Kundenkontakt in seiner Zukunft als Berater für Informationssicherheit und Datenschutz.

Ein Informatiker auf der nicht-wissenschaftlichen Berufslaufbahn

Während die meisten seiner Kommiliton:innen als Informatik-Absolventen eine wissenschaftliche Laufbahn einschlagen, wurde ihm bereits während seines ersten Praktikums in den Semesterferien bei der DATATREE AG klar, dass ihm der Kontakt zu Kund:innen gefällt. Er wurde langsam an die Themen herangeführt, hat sich bei der Entwicklung von Datenschutzkonzepten beteiligt und bei Förderprojekten mitgewirkt. „Für mich ist es optimal, meinen akademischen Schwerpunkt im Bereich Informationssicherheit durch die Praxis in Verbindung mit Kund:innen zusammenbringen zu können", zieht Niklas das Fazit über seine berufliche Entscheidung.

Es lässt sich also festhalten: Routinen sind für den einen obligatorisch und für den anderen hilfreich. Aber sie sind nicht zwingend ein Bestandteil des Jobs.

Was für Andreas und Niklas im persönlichen Ermessen liegt, wurde für Sina Rochow-Pahl im Laufe des letzten Jahres zur Notwendigkeit: Die 32-Jährige ist Mutter geworden und kehrte Anfang Juli wieder als Beraterin für Datenschutz zur DATATREE AG zurück. „Natürlich ist das eine große Umstellung", sagt Sina, „mit einem Baby ist logischerweise erst mal jegliche Spontaneität verflogen. Es ergeben sich automatisch Routinen, die ich nicht nur als hilfreich empfinde, sondern die ich sogar benötige, um Familie und Job unter einen Hut zu bringen. Dazu gehört beispielsweise die Umstellung auf einen festgelegten Essens- und Schlafrhythmus beim Baby."

Familie und Beruf meistern: *Sina Rochow-Pahl*

Was ebenfalls entsteht, ist eine gewisse Inflexibilität bei den Arbeitszeiten: „Vor meiner Schwangerschaft habe ich viel gearbeitet und konnte mich voll und ganz auf Projekte mit Kund:innen einlassen. Termine am späten Nachmittag waren da immer problemlos möglich", berichtet Sina, „das ist jetzt natürlich anders – meine Arbeitszeiten und damit einhergehende Termine müssen von mir nun gut geplant und koordiniert werden. Da ich für die Koordination mit meinen Kund:innen eigenverantwortlich tätig bin, ist das DATATREE Team offen für diese Umstellung, in der man in der Doppelrolle als berufstätige Mutter wieder in den Job zurückkehrt. Die Familienzeit wird berücksichtigt, sodass ich meine berufliche Tätigkeit hiermit gut kombinieren kann." So führt sie Termine entweder remote durch oder plant Meetings vor Ort mit Kund:innen im Voraus, damit es ihr Zeitplan zulässt.

Im Büro ist sie zweimal pro Woche, die restliche Arbeitszeit leistet sie aus dem Homeoffice. Mit ihrem Teamlead stimmt sie individuell ab, wann sie im Dortmunder Büro ist. Zwar sei sie gedanklich auch nach der Arbeitszeit immer mal wieder bei Projekten, insgesamt empfindet Sina aber die Vereinbarkeit von Familie und Beruf bei der DATATREE AG als gut umsetzbar – auch, dank eigens gewählter Routinen.

> *Das eigenverantwortliche Strukturieren meines Arbeitstages ermöglicht die Vereinbarkeit von Familie und Beruf.*
>
> Sina Rochow-Pahl
> *Beraterin Datenschutz*

Die Psychologie zwischen Notwendigkeit und Orientierung

Ein Interview mit Rechtspsychologin Laura Kill.

In jeder Person stecken Routinen. Gewohnte Abläufe gelten als Erleichterung. Über Gelerntes müssen wir wenig nachdenken und das spart dem Gehirn Energie und Zeit. Und die wiederum lässt sich hervorragend in produktive, aufregende und neue Dinge investieren. Aber wie sieht es bei Menschen aus, die diese Möglichkeit nicht haben?

Fernab von Digitalisierung, Informationssicherheit und Datenschutz haben wir dieses Mal den Blick über den Tellerrand gewagt und eine Rechtspsychologin befragt, wie es um Routinen von Gefangenen in einem Justizvollzug bestellt ist – und wie sehr sich diese von Nichtgefangenen unterscheiden.

ExperSite *Laura, bitte erzähle uns kurz etwas von Dir und Deiner Tätigkeit im Vollzug.*

Laura Kill: Ich arbeite als Rechtspsychologin im Justizvollzug mit weiblichen, jungen Gefangenen in der Untersuchungs- sowie Strafhaft. Das Ziel meiner Arbeit ist es, die Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen. Für die Mitarbeitenden des psychologischen Dienstes fächert sich die Arbeit besonders in zwei Aspekte auf: Diagnostik und Behandlung. Diagnostik umfasst unter anderem Stellungnahmen für vollzugsöffnende Maßnahmen und Abklärung möglicher suizidaler Gefährdungsmomente. Behandlungen können Gruppenmaßnahmen und Einzelgesprächsreihen sein.

ExperSite *Welche Rolle spielen Routinen für Dich persönlich, um Deine Arbeit durchführen zu können?*

Laura Kill: In meinem Arbeitstag spielen Routinen eine wichtige Rolle. Das bezieht sich auf konkrete Arbeitsabläufe und auch auf komplexere Aspekte. Im Vollzug spiegeln sich Routinen für jede:n Bedienstete:n vor allem in Sicherheitsaspekten wider. Als ganz banales Beispiel dient da das Öffnen und Verschließen jeder Tür. Das läuft automatisiert ab und betrifft alle Bediensteten. Für mich als Psychologin gibt es routinemäßig in der Untersuchungshaft bei jedem Gespräch auch immer eine Einschätzung darüber, ob eine Person suzidial erscheint und entsprechende Sicherungsmaßnahmen zum Schutz der körperlichen Unversehrtheit getroffen werden müssen.

ExperSite *Wie sieht es mit der Relevanz von Routinen für Deine Klient:innen im Vollzug aus - inwieweit hilft ihnen ein routinierter Ablauf, um den Alltag zu bestreiten?*

Laura Kill: Für die Gefangenen bieten die Routinen im Vollzug Sicherheit und Kontinuität. Es ist wichtig, den Gefangenen Verlässlichkeit vorzuleben. Ein Aspekt, der in der Vergangenheit bei den jungen Gefangenen durch die Eltern oftmals vernachlässigt wurde. Nicht ohne Grund zählt Verlässlichkeit in zwischenmenschlichen Beziehungen als wichtiges Motiv, was unser Klientel bedarf und was kontinuierlich gestillt werden muss. Das erreichen wir im Vollzug durch Routinen, die sich vielfältig gestalten: Kostausgabe, Verschlusszeiten, Einkauf, Schul- und Ausbildungsbesuch und für mich im Besonderen: feste Gesprächszeiten.

ExperSite *Kann jede:r Routinen erlernen?*

Laura Kill: Das Erlernen von Routinen ist ein wichtiger Aspekt der Erziehung und setzt sich im Leben weiter fort. Jede Person, die ein Unternehmen gewechselt hat, musste sich zu Beginn der Tätigkeit mit den im Unternehmen vorhandenen, sich wiederholenden Handlungen auseinandersetzen, sich diese aneignen und automatisieren. Die Wiederholung dieser Handlungen schafft dabei Automatismen. Dabei ist es aus psychologischer Sicht natürlich immens wichtig, in diesen Handlungen einen Nutzen bzw. ein Ziel zu sehen, sonst wird daraus nur schwer ein Automatismus.

> „Routinen sichern für alle Beteiligten im Vollzug die Abläufe

Viele Entscheidungssituationen, denen wir in natürlichen Kontexten begegnen, sind dadurch gekennzeichnet, dass sie sich wiederholen. Dazu zählt der Weg zur Arbeit, was wir frühstücken, wie wir unseren Abend gestalten. Über Erfahrungen lernen wir, welche Handlungsalternativen in bestimmten Situationen zu vermeiden sind und vor allem, welche Alternativen gute Lösungen für ein Entscheidungsproblem darstellen. So erwerben wir schließlich Routinen für wiederkehrende Entscheidungssituationen.

Bei neuen Entscheidungsproblemen ist uns die Lösung - also ein zielführendes Verhalten - anfangs unbekannt. Wir müssen uns mit den verfügbaren Alternativen auseinandersetzen, sie bewerten und schließlich eine Wahl treffen. Bei neuen Entscheidungen geht es darum, eine Lösung für das Problem zu identifizieren. Abstrakt formuliert lässt sich im Hinblick auf Routinen sagen, dass routinierte Entscheidungen dort beginnen, wo diese neuen Entscheidungen aufhören. Die Identifikation einer möglichen Lösung für ein Problem steht dabei am Anfang des Entscheidungsprozesses. Damit verändert sich jedoch auch die Struktur eines Problems. Bei neuen Entscheidungen geht es um die Frage „Welches Verhalten soll ich wählen?“ Bei routinierten Entscheidungen lautet die zugrunde liegende Fragestellung „Soll ich mein bisheriges Verhalten beibehalten oder davon abweichen?“

> Aus psychologischer Sicht ist es immens wichtig, in Handlungen einen Nutzen bzw. ein Ziel zu sehen, sonst wird daraus nur schwer ein routinierter Automatismus.
>
> LAURA KILL
> *Rechtspsychologin, M.Sc.*

Für das Klientel im Vollzug ist es, wie für jede andere Person auch, möglich, Routinen zu erlernen. Hier im Vollzug sichern sie für alle Beteiligten die Abläufe. Das betrifft sowohl Sicherheitsaspekte, als auch die Gestaltung von ressourcenschonenden Abläufen. Für die jungen Menschen geht es darum, einen Nutzen in den Routinen zu sehen: für sich selbst, für die Gemeinschaft und für die gesamte Anstalt. Werden verschiedene Routinen missachtet, folgen daraus Konsequenzen und je nach Schweregrad auch anschließende Sanktionen. Und wenn die Gefangenen merken, dass die Kosten ihres Verhaltens langfristig den Gewinnen im Weg stehen, kann dies auch zu einer funktionaleren Verhaltensänderung führen.

ExperSite ***Und wenn sie den geschützten Raum der JVA verlassen?***

Laura Kill: Hier geht es auch wieder um die Aspekte der Entscheidungsfindung. Sie sollen ja nicht nur auf konkrete Abläufe bezogen werden, die nach einer Entlassung für den Tagesablauf nicht mehr sinngemäß sind. Wenn wir Routinen weiter fassen, bezieht es auch deliktpräventive Faktoren mit ein, z. B. einen angemesseneren Umgang mit Negativentscheidungen, bei Provokationen gelassener zu reagieren oder funktionale Strategien bei erhöhter Impulsivität zu implementieren. Wenn wir uns im störungsspezifischen Bereich bewegen, z. B. bei der emotional-instabilen Persönlichkeitsstörung, dann sind sogenannte „Skills" - also Verhaltensweisen - zum Spannungsabbau, routinemäßig zu etablieren. Bildhaft formuliert erarbeiten wir mit den jungen Menschen hier ihren eigenen Werkzeugkasten, bestärken sie darin für spezifische Situationen das passende „Werkzeug" zu nutzen. Dabei helfen Routinen ungemein.

ExperSite ***Bleiben einmal erlernte Routinen in einem neuen Umfeld existieren oder müssen diese neu erlernt werden?***

Laura Kill: Wenn die zuvor erlernten Routinen auch weiterhin Bestand haben, können diese sich weiter verfestigen. Die kognitive Repräsentanz im Gehirn ist vorhanden. Sie kann aber auch auf neue Umstände adaptiert werden. Der Mensch denkt dabei sehr assoziativ, ist aber durchaus in der Lage, sich an neue Gegebenheiten anzupassen und neue Routinen auszuprägen.

ExperSite ***Was ist der Unterschied zwischen einer Routine und einem Zwang?***

Laura Kill: Mit Routinen sind bestimmte Handlungsabfolgen gemeint, die anfangs vielmals wiederholt werden, bis sie schlussendlich eine Gewohnheit sind. Wichtig ist dabei der Aspekt, dass diese Handlungsabfolgen einen Nutzen haben. Zwänge beinhalten starke, wiederkehrende Impulse, die Menschen zu Handlungen „zwingen" und es schwer bis unmöglich machen, diesen zu widerstehen. Wir reden hier von einer psychischen Störung, die Betroffene in ihrer alltäglichen Lebensführung stark einschränken und Leidensdruck verursachen. Sie haben permanent das Gefühl, sie müssten diesen Impulsen nachgeben. Der innere Widerstand, die Handlungen oder Gedanken zu unterlassen, kostet viel Kraft und erzeugt immer stärker werdende Anspannung und Angst. Erst, wenn sie den Zwängen nachgeben, lässt der Druck nach, bevor sich der Zwangsgedanke erneut aufdrängt.

ExperSite ***Können sich aus Routinen Zwangsstörungen entwickeln?***

Laura Kill: Ritualisierende Abläufe und alltägliche Routine geben uns Sicherheit und Struktur im Alltag. Was Zwänge von alltäglichen, wiederkehrenden Ritualen unterscheidet, ist, dass unerwünschte Gedanken und Handlungen immer mehr Zeit beanspruchen und zunehmend einen Leidensdruck bei den Betroffenen auslösen bzw. deren Alltag beherrschen. Zudem wissen die Betroffenen meist um die Unsinnigkeit von Zwangsgedanken bzw. -handlungen, sind aber nicht in der Lage, auf die kurzfristig erleichternd wirkenden ritualisierten Handlungen zu verzichten. Zwänge können also trotz Einsicht und Vernunft kaum unterdrückt werden.

> Zwangsstörungen sind meistens mit Ängsten verbunden

Sie dienen in erster Linie dazu, Sicherheit zu schaffen und Probleme zu lösen, die für die Erkrankten auf keine andere Weise zu bewältigen sind. Bei der Entstehung und Aufrechterhaltung einer Zwangserkrankung spielen nach heutiger Erkenntnis immer mehrere Faktoren eine Rolle – psychologische und biologische. Dabei ist es individuell unterschiedlich, welche der einzelnen Faktoren in welchem Ausmaß relevant sind. Familienuntersuchungen und Zwillingsstudien zeigen, dass es – wie bei den meisten psychischen Erkrankungen – eine erbliche Vorbelastung für die Zwangsstörung gibt. Damit sie ausbricht, müssen jedoch weitere Faktoren hinzukommen. Dazu gehören beispielsweise Erfahrungen in der Kindheit, die dazu geführt haben, dass ein Mensch eher unsicher ist und ein stärkeres Kontrollbedürfnis hat. Bei mehr als der Hälfte der Betroffenen ist die Erkrankung mit Stress oder mit einem schwerwiegenden Lebensereignis verbunden.

ExperSite ***Sind Routinen also eher etwas Gutes oder etwas Schlechtes?***

Laura Kill: Reden wir von Zwangshandlungen, über deren Unsinnigkeit wir uns bewusst sind, die wir jedoch nicht abstellen können, bewegen wir uns im Störungs-Bereich, der einer Behandlung bedarf. Hinter Zwangserkrankungen stecken Ängste, die wir versuchen, durch den Zwang abzumildern. Heruntergebrochen ist die Intention kurzfristig gut, die Umsetzung jedoch sehr ressourcenintensiv. Wenn wir an einer Suchterkrankung leiden, wie z. B. Zigarettenkonsum, dann erschweren uns Routinen, wie die morgendliche Zigarette beim Kaffee, das Aufhören. Diese Routinen müssten zuerst durchbrochen werden, wenn wir nicht von 100 auf 0 direkt abstinent sein können. Sprechen wir aber über automatisch ablaufende Routinen, die wir für unseren Alltag geschaffen haben, sind sie etwas Gutes. Sie erleichtern uns den Alltag und bestimmte Abläufe, im Privaten oder Beruflichen. Dabei spielt es keine Rolle, ob wir Gefangene in einem Vollzug sind oder nicht.

Laura Kill berichtet im Interview mit ExperSite über Routinen von Gefangenen in einem Justizvollzug.

DATATREE PRÜFGEMEINSCHAFT

Erfolgreich Synergien schaffen

KRITIS, die Datenschutzgrundverordnung, das Sozialgesetzbuch oder auch die Norm ISO 27001 haben eines gemeinsam: Sie machen die Prüfung von AV-Dienstleister:innen (Dienstleister:innen, die im Auftrag agieren) in Form von Dienstleister-Audits zwingend erforderlich.

Für Krankenkassen stellt das jedoch eine enorme organisatorische, personelle und finanzielle Herausforderung dar. Deshalb bietet die DATATREE AG als langjährige Dienstleisterin in den Bereichen Informationssicherheit, Compliance und Datenschutz die Durchführung in Form einer gemeinschaftlichen Prüfung – der Prüfgemeinschaft - an.

Sie führt für Krankenkassen die vollständige Planung und Abwicklung von Audits in den Bereichen Informationssicherheit und Datenschutz durch langjährig erfahrene und branchenkompetente Auditoren durch und übernimmt Prozessprüfungen, Begehungen, Verfahrenschecks sowie Risikoeinschätzungen und deren Bewertungen. Die Koordination und Teilnahmeerklärung zu Dienstleister-Audits sowie die Bereitstellung von Prüfberichten und Follow-Up-Meldungen werden transparent über ein Webportal organisiert.

Im vergangenen Jahr wurden auf diese Weise 22 Prüfungen erfolgreich durchgeführt und mehr als 30 Krankenkassen entlastet.

Durch die gemeinschaftliche Prüfung entstehen Kostensynergien, da sich die Aufwände auf alle Teilnehmenden an einem Audit gleichermaßen aufteilen. Anstatt vielfacher Prüfungen durch die einzelnen Einrichtungen/Auftraggeber:innen ist regelmäßig nur eine Auditierung notwendig.

Die Prüfgemeinschaft hat sich zu einem Netzwerk entwickelt. Halbjährliche Treffen werden nicht nur zum Erfahrungsaustausch genutzt, sondern auch zu Fortbildungszwecken im Bereich des Datenschutzes und der Informationssicherheit im Sinne der Anforderung gemäß Art. 38 Abs. 2 DSGVO.

Sie haben ebenfalls Interesse, Teil der Prüfgemeinschaft zu werden? Dann wenden Sie sich gerne an
nina.kill@datatree.ag

WIR SIND DIE JÄSCHKE GRUPPE

Gemeinsam Digitalisierung leben

Unsere interdisziplinären Kompetenzen sind unser unternehmerisches Kapital. Trotz unterschiedlicher Schwerpunkte haben wir als Unternehmensgruppe ein gemeinsames Ziel:

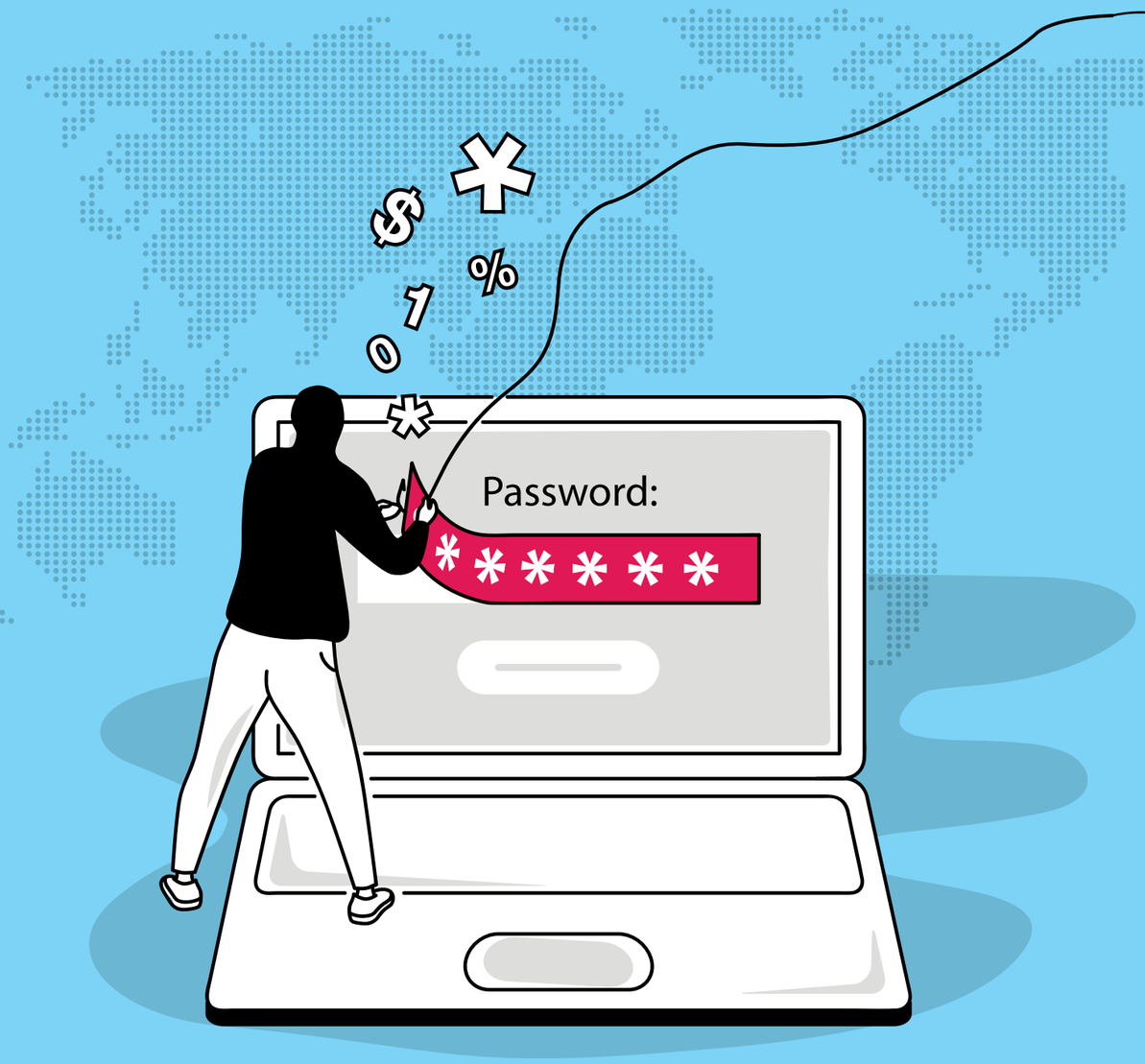
Ob Management Consultant, IT-Expert:in oder Datenschutzspezialist:in - Wir unterstützen Sie bei Ihren digitalen Herausforderungen. Wir bilden Strategien, die auf den digitalen Reifegrad Ihres Unternehmens abgestimmt sind und wir wissen, was wir tun - dank unserer Vielseitigkeit ohne Improvisation, sondern mit Know-how und Erfahrung.

www.dr-jaeschke.ag

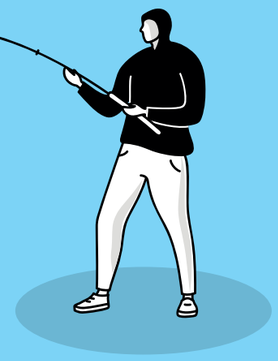
Sind Sie bereit für Ihren digitalen Wandel? Lassen Sie uns gemeinsam Ihren Prozess beginnen.

JÄSCHKE GRUPPE
GEMEINSAM DIGITALISIERUNG LEBEN

Wie erstelle ich eine Passwortrichtlinie?



Sichere Passwörter sind für den Schutz unserer IT-Systeme und vor allem der personenbezogenen Daten, die wir verarbeiten, von elementarer Bedeutung. Eine Passwort-Richtlinie bildet hierzu die Grundlage für Ihr Unternehmen und beschreibt verbindlich die Mindestanforderungen an die Qualität von Passwörtern und die Regeln im Umgang mit ihnen.



Eine Richtlinie allein wird nicht automatisch zu optimalen Passwörtern führen, denn nach wie vor sind wir Menschen die größte Schwachstelle. Damit ein Passwort als sicher gilt und eine Passwortrichtlinie effektiv eingeführt werden kann, sollten ein paar simple Regeln eingehalten werden.

Wir geben Ihnen drei Aspekte an die Hand, die in keiner Passwortrichtlinie fehlen sollten.

1 Rahmenbedingungen einer wirksamen Passwortrichtlinie festlegen

Mit diesen Tipps gelingt es Ihnen, einheitliche Rahmenbedingungen für Ihre Passwort-Richtlinie zu schaffen:

- Eine Passwort-Richtlinie sollte klar und verständlich für alle sein. Vermeiden Sie technische und juristische Fachsprache, damit alle Nutzer:innen Sie verstehen können.
- Veröffentlichen Sie die Passwort-Richtlinie im Mitarbeitendenhandbuch oder im Intranet, damit sie für alle leicht zugänglich ist.
- Stellen Sie sicher, dass die Passwort-Richtlinie immer auf bewährten Maßnahmen basiert, zum Beispiel auf der Verwendung eines Passwortmanagers oder der Zwei-Faktor-Authentifizierung.
- Richten Sie die Passwort-Richtlinie so ein, dass sie keine häufig wechselnden Passwörter oder Sicherheitsfragen erfordert.
- Die Passwortrichtlinie dient der IT-Abteilung als zentrale Möglichkeit, die Passwortsicherheit im Unternehmen zu verwalten und zu überwachen.
- Sollte sich die Bedrohunglage ändern, ist die IT-Abteilung die richtige Stelle, um die Passwort-Richtlinie zu aktualisieren.
- Eine Passwort-Richtlinie ist für alle da. Sie sollte deshalb regelmäßig den Mitarbeitenden in Schulungen nahegebracht werden.
- Achten Sie darauf, dass die Passwort-Richtlinie effektiv umgesetzt und vor allem regelmäßig überwacht wird. Änderungen gilt es gegebenenfalls einzuarbeiten.

2 Formale Anforderungen an Passwörter bestimmen

Wir alle wissen, wie schwierig es ist, sich immer wieder neue Passwörter für all die verschiedenen Dienste auszudenken, die wir heutzutage nutzen. Um Ihre Mitarbeitenden zu unterstützen, sollten ihnen folgende formale Anforderung vorgegeben werden:

- Je länger das Passwort ist, desto sicherer ist es: Geben Sie eine Mindestlänge von 8 Zeichen vor. Für WLAN wie zum Beispiel WPA2 oder WPA3 sollte das Passwort sogar 20 Zeichen haben.
- Für Passwörter können alle verfügbaren Zeichen genutzt werden: Groß- und Kleinschreibung, Ziffern und Sonderzeichen. Mindestens drei dieser vier Anforderungen müssen erfüllt sein, um das Passwort möglichst sicher zu machen.
- Ein vollständiges Passwort sollte nicht im Wörterbuch vorkommen, weil Hacker es relativ schnell durch einen sogenannten Wörterbuchangriff entschlüsseln können. Passwörter wie „password", „iloveyou" oder „admin" sind also tabu.
- Wenig originell und ebenso leicht von Hackern zu knacken sind gängige Zahlenfolgen (z.B. 123456789) oder Tastaturmuster (z.B. asdfgh). Auch hier gilt: Diese Passwörter werden besser nicht gewählt.
- Noch ein Klassiker: Namen von Familienmitgliedern, Haustieren, Freunden oder Geburtsdaten. Lassen Sie Ihre Mitarbeitenden wissen, dass das keine gute Wahl ist.
- Die Ergänzung von einfachen Ziffern oder Sonderzeichen nach einem „normalen Wort", also einem Wort aus dem Wörterbuch, ist ebenfalls nicht zu empfehlen. Jeder Mitarbeitende sollte wissen, dass zum Beispiel „admin!" kein sicheres Passwort ist.
- Um die Sicherheit zu erhöhen: Aktivieren Sie die Zwei-Faktor-Authentifizierung[1].
- Die gleiche Kombination von Benutzername und Passwort für verschiedene Dienste sollte nie verwendet werden! Die wichtigsten Passwörter sollten immer individuell und stark sein.

Generell sollten Sie auch den direkten Umgang mit Passwörtern in der Richtline deutlich machen und Ihre Mitarbeitenden durch Schulungen sensibilisieren:

- Geben Sie Passwörter nicht an Dritte weiter und versenden Sie sie nicht per E-Mail!
- Bewahren Sie Ihre Passwörter nicht in der Nähe Ihres Schreibtischs auf, falls Sie sie noch auf Papier festhalten.
- Ersetzen Sie voreingestellte Passwörter umgehend durch ein persönliches!

3 Technische Anforderungen für Ihre IT-Abteilung definieren

Ihre IT-Abteilung kann durch bestimmte Vorkehrungen dafür sorgen, dass der Missbrauch von Passwörtern zumindest erschwert, im besten Falle natürlich gar nicht erst ermöglicht wird. Durch folgende Maßnahmen setzen IT-Mitarbeitende die Standards, um unerwünschte Eingriffe zu vermeiden:

Änderungsintervall festlegen:

- Sollte der Verdacht bestehen, dass das Passwort unbefugten Dritten bekannt sein könnte, ist es zwingend sofort zu ändern!
- Zu Empfehlen ist das Festlegen einer Passwort-Historie[2]: Empfehlung: Die letzten zehn Passwörter sollten nicht wiederverwendet werden.
- **Anzahl falscher Anmeldeversuche festlegen:**
  1. Beispiel: Zehn Versuche bis zum Sperren der Kennung des Benutzers/der Benutzerin
  2. Beispiel: Fünf Versuche bis zum Sperren der Kennung des Benutzers/der Benutzerin + automatisches Entsperren durch das System/der Anwendung nach 30 Minuten
  3. Beispiel: Drei Versuche bis zum Sperren der Kennung des Benutzers/der Benutzerin + Freigabe durch ein Administratorpasswort
- Konfigurieren Sie ergänzend zur Passworthistorie ein minimales Passwortalter. Auf diese Weise wird vermieden, dass Benutzer ihre Passwörter in kurzer Zeit mehrmals ändern und sie dadurch versehentlich oder absichtlich alte Passwörter verwenden.

[1] Die Zwei-Faktor-Authentisierung gibt es in mehreren Varianten, einige ergänzen das zuvor eingegebene Passwort um einen zusätzlichen Faktor, andere ersetzen das vorherige Log-In mit Passwort komplett durch eine direkte Kombination zweier Faktoren. Dabei bieten vor allem hardwaregestützte Verfahren ein hohes Maß an Sicherheit und sollten ergänzend/ersetzend zu einem starken Passwort genutzt werden.

[2] Die Passworthistorie beinhaltet die letzten Passwörter. Der Benutzer/die Benutzerin kann diese so lange nicht wiederverwenden, bis diese nicht mehr in der Passworthistorie stehen.

NICE TO KNOW
Passwortmanager

Um die Akzeptanz der Mitarbeitenden für strikte Passwortregularien zu stärken, wird generell der Einsatz von Passwortmanagern empfohlen. Hierbei muss sich nur ein einziges Passwort, das Masterpasswort, gemerkt werden. Passwörter für verschiedene Dienste können durch den Passwortmanager generiert werden. Ebenfalls gibt es die Möglichkeit, sich die Sicherheitsstufe des Passworts auszusuchen, je nachdem, wie stark der Passwortschutz sein soll. Außerdem können die generierten Passwörter in dem Passwortmanager gespeichert werden.

Vorteile Einbindung Passwort-Manager:

- **Mittels Verschlüsselung werden Passwörter verwahrt**
- **Hilfe bei der Passwortvergabe:** z. B. durch die Generierung starker Kombinationen und Kennzeichnung schon verwendeter oder schwacher Begriffe.
- **Warnung vor gefährdeten Websites und möglichen Phishing-Attacken**, z. B. wenn sich die URL der aufgerufenen Webseite von der gespeicherten unterscheidet.
- **Synchronisieren möglich,** wenn Online-Dienste auf mehreren Geräten wie Computer und Smartphone mit unterschiedlichen Betriebssystemen genutzt werden.

Nachteile Einbindung Passwort-Manager:

- Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren: Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen.
- Bei einem Cyber-Angriff auf den Passwort-Manager können alle Passwörter auf einmal gestohlen werden.
- Es sollten grundsätzlich die AGB und Datenschutzerklärungen geprüft werden, insbesondere bei cloudbasierten Diensten. Vor allem im Hinblick auf den Unternehmensstandort des Cloud-Dienst-Anbieters und den Standort des Servers, welcher zusätzlich Informationen darüber gibt, welchem Datenschutzrecht die Daten unterworfen sind.

Die Einführung einer einheitlichen Passwortrichtlinie, um die Sicherheit der IT-Systeme zu gewährleisten, ist für ein Unternehmen eine große Herausforderung. Mit den oben aufgeführten Aspekten und Empfehlungen wird Ihnen und Ihren Mitarbeitenden der Einstieg zur optimalen Umsetzung erleichtert. Nur das Zusammenspiel aus allen Aspekten stellt starke Passwörter und somit ein hohes Sicherheitsmaß in Ihrem Unternehmen sicher.

Die Angaben entsprechen den aktuellen Standards des BSI.

Über die Autorin Kim Kurzhals:
Kim Kurzhals ist seit Juli 2021 als Beraterin im Bereich Datenschutz bei der DATATREE AG angestellt. Zuvor absolvierte Sie ihr Masterstudium im Bereich Wirtschaftsrecht an der Westfälischen Hochschule. Durch Ihr fachliches Know-how gehören u.a. AV-Verträge zu ihrem Spezialgebiet.

CONSENT-BANNER

Wer blickt hier noch durch?

Wir surfen im Internet, möchten durch beliebige Webseiten stöbern und plötzlich erscheinen diese mehr oder weniger nervenzerreißenden Consent-Banner, durch die wir uns erst hindurchklicken müssen. Auffällig ist dabei, dass sämtliche Cookies durch nur einen Klick akzeptiert werden können.

Meistens erfolgt dieser Klick auf einem optisch hervorgehobenen Button. Möchte man die Cookies jedoch ablehnen, steht man vor einer Herausforderung und muss sich zunächst durch verschiedene Einstellungen kämpfen.

Um uns diese Mühe zu ersparen, wählen wir doch lieber den einfacheren Weg: Wir klicken auf den optisch hervorgehobenen „Akzeptieren"-Button und nehmen sämtliche Cookies in Kauf. Diese Entscheidung haben wir unbewusst durch das so genannte „Nudging" seitens des jeweiligen Webseitenbetreibenden getroffen.

> Wir klicken auf den optisch hervorgehobenen „Akzeptieren"-Button und nehmen sämtliche Cookies in Kauf.

Was bedeutet „Nudging" und wie funktioniert es?

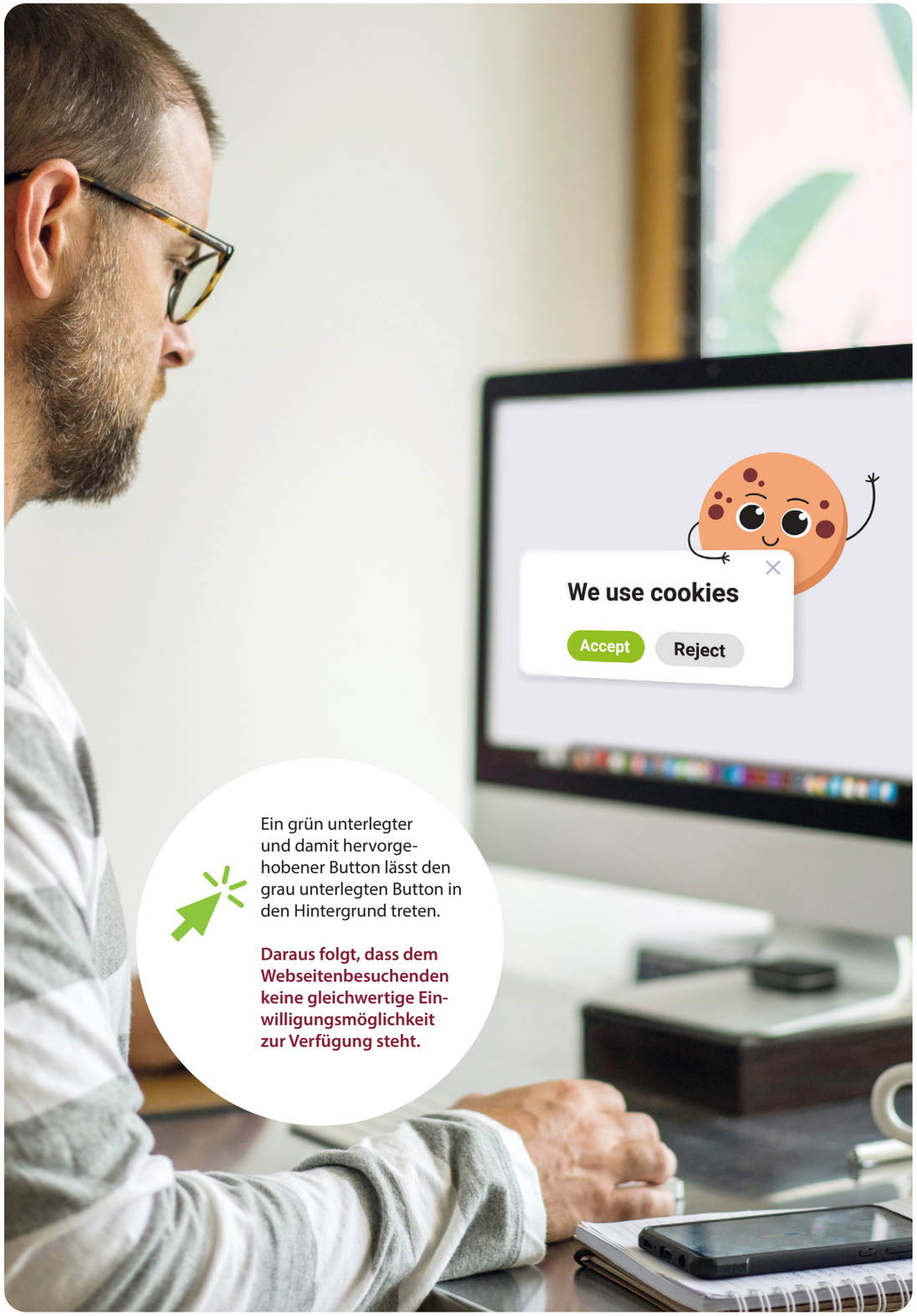
Nudging ist ein Begriff aus der Verhaltensökonomik und leitet sich aus dem englischen Begriff „nudging", für „anstoßen", „schubsen" oder „stupsen" ab.

Es handelt sich dabei um eine Strategie zur Verhaltensänderung des Menschen.

Mit anderen Worten: Diejenigen, die Nudging betreiben, möchten den Menschen auf eine mehr oder weniger subtile Weise beeinflussen, etwas Bestimmtes einmalig oder dauerhaft zu tun oder zu lassen. Handlungsoptionen sollen nicht verboten werden, vielmehr soll die Entscheidung in Richtung einer von mehreren Entscheidungsoptionen gelenkt werden. Nudging existiert in unterschiedlichen Konstellationen: digitale Design-Muster, Voreinstellungen oder auch vorausgewählte Auswahlkästchen fallen darunter.[1]

In unserem Fall setzen also die Webseitenbetreibenden Nudging durch die grafische Darstellung ihres Consent-Banners ein. Sie bewegen uns durch ein bestimmtes Design zu einer bestimmten Entscheidung - durch die eingesetzte Farbe, Größe und Position des „Akzeptieren"- und/oder „Ablehnen"-Buttons wird uns suggeriert, auf welchen Button wir klicken sollen.

[1] ZD 2021, 404, Rn. 404.



Ein grün unterlegter und damit hervorgehobener Button lässt den grau unterlegten Button in den Hintergrund treten.

Daraus folgt, dass dem Webseitenbesuchenden keine gleichwertige Einwilligungsmöglichkeit zur Verfügung steht.

Ist Nudging überhaupt im Sinne des Datenschutzes?

Eine ausdrückliche gesetzliche Regelung zu Nudging existiert bislang nicht. Die Grenze zwischen einer rechtlich noch akzeptablen Lenkung und einer rechtlich verbotenen Manipulation lässt sich nicht abschließend ziehen. Problematisch ist dies insbesondere für das Datenschutzrecht, wie nur zwei Punkte von vielen verdeutlichen:

• Fehlende Wirksamkeit der Einwilligung

Mit Einführung des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) ist der Einsatz von technisch nicht notwendigen Technologien, wie z.B. Cookies oder sämtlichen Analysetools, durch die Webseitenbetreibenden nur erlaubt, wenn eine vorherige Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO i.V.m. § 25 Abs. 1 TTDSG eingeholt wurde.

Die Einwilligung gem. Art. 7 Abs. 1 DSGVO ist eine in informierter Weise unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist.

Das Landesgericht Rostock hat im Urteil vom 15.09.2020, Az. 3 O 762/19, diesbezüglich Stellung genommen und entschieden, dass **keine** informierte und freiwillige Einwilligung vorliegt, wenn in Form des Nudgings eine Einwilligung über den Consent-Banner herbeigeführt wurde. Zwar hat der Webseitenbesuchende die Möglichkeit, die Details zu den einzelnen Cookies aufzusuchen und abzuwählen. Mit hoher Wahrscheinlichkeit wird er regelmäßig den Aufwand eines solchen Vorgehens jedoch scheuen und deshalb den hervorgehobenen „Akzeptieren"-Button bestätigen. Ohne die erforderliche vorherige Information über die Details kann der Webseitenbesuchende nicht wissen, welche Tragweite seine Erklärung beim Anklicken des „Akzeptieren"-Buttons hat.

• Verstoß gegen den Transparenzgrundsatz

Zusätzlich tritt im Rahmen des Nudgings der Verstoß gegen den Transparenzgrundsatz auf. Laut des Erwägungsgrundes 58 in der DSGVO setzt der Grundsatz der Transparenz voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information **präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abzufassen ist.** Daraus folgt, dass das Abwählen der einzelnen, technisch nicht notwendigen Cookies nicht schwieriger sein darf als das Annehmen. Sobald wir uns erst durch verschiedene Einstellungen begeben müssen oder uns nicht bewusst ist, wie und wo wir die Cookies abwählen können, kann von Transparenz nicht mehr die Rede sein.

Auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat in einer Orientierungshilfe vom 20.12.2021 klargestellt, dass Consent-Banner auf Webseiten als Alternative zur Zustimmung ebenfalls einen Button aufzeigen müssen, der gleich schnell zur gewünschten Nutzung der Webseite führt. Die Möglichkeit zur Abwahl- und Annahme muss den gleichen kommunikativen Effekt haben. Daran mangelt es, wenn man indirekt durch den Webseitenbetreibenden in eine gewünschte Richtung durch eine farbliche Markierung „gedrängt" wird.

Fazit

Die irreführenden Consent-Banner vermitteln den Besuchenden der Webseite fälschlicherweise den Eindruck, dass dies dem Datenschutz geschuldet ist.

Im Gegenteil (!): Der Datenschutz verlangt die Einführung einer einfachen Wahlmöglichkeit zugunsten der Webseitenbesuchenden.
Webseitenbetreibende sollten sich an die rechtlichen Anforderungen eines Consent-Banners halten, da das Urteil des LG Rostock sowie die zunehmenden Abmahnverfahren verdeutlichen, das Nudging in Consent-Bannern nicht länger geduldet wird. Festzuhalten ist somit, dass das Nudging im Zusammenhang mit Consent-Bannern nicht im Sinne des Datenschutzes ist.

10 Tipps, die Websitebetreibende bei der Erstellung Ihres Consent-Banners beachten sollten:

1. Stellen Sie als Webseitenbetreibende/r den Consent-Banner selbst bereit. Sollten Sie ein Consent-Management-Tool eines externen Anbietenden nutzen, ist die Benennung dieses Anbietenden im Constent-Banner erforderlich.
2. Bieten Sie eine einfache Wahlmöglichkeit an, damit Besuchende Ihrer Webseite für das Ablehnen der Cookies keine zweite Seite aufrufen müssen. „Anpassen"-Buttons, die erst im zweiten Schritt zur Ablehnung von Cookies führen, sollten Sie vermeiden.
3. Achten Sie auf eine klare und einfache Sprache und verwenden Sie keine irreführenden Buttons, die nicht zur gewünschten Auswahl führen.
4. Heben Sie den „Akzeptieren"-Button nicht hervor, sondern wählen Sie die gleiche Farbe, Größe und Position wie für den „Ablehnen"-Button.
5. Verwenden Sie keine Voreinstellungen oder bereits ausgewählte Auswahlkästchen.
6. Binden Sie sämtliche Cookies und eingesetzte Tracking- und Analysetools im Consent-Banner ein.
7. Cookies, die technisch nicht erforderlich sind und eingesetzte Tracking- und Analyse-Tools, dürfen nicht hinter „allgemeinen" Überschriften wie z.B. „Marketingzwecke" oder „Forschungszwecke" versteckt werden.
8. Setzen Sie technisch nicht notwendige Technologien erst ein, wenn der/die Webseitenbesuchende eine vorherige Einwilligung abgegeben hat.
9. Die Umsetzung eines „Cookie-Einstellungen"-Buttons in der Fußzeile der Webseite ist zu empfehlen, um dem/der Webseitenbesuchenden die Möglichkeit anzubieten, nachträglich den Consent-Banner aufzurufen und seine/ihre Auswahl abzuändern.
10. Mit Einführung des Consent-Banners sollte durch die IT-Abteilung eine nachträgliche Kontrolle erfolgen, um sicherzustellen, dass technisch nicht erforderliche Cookies sowie Tracking- und Analyse-Tools trotz einer Ablehnung nicht angewendet werden.

Let´s do it.

Über die Autorin Bahar Sediqi:
Bahar Sediqi ist seit Juni 2021 als Beraterin im Bereich Datenschutz bei der DATATREE AG tätig. Die Wirtschaftsrecht-Absolventin ist für die Einführung von Datenschutz-Managementsystemen zuständig und gibt regelmäßig Schulungen zu datenschutzrechtlichen Themen.

Literatur
Loy/Baumgartner:
Consent-Banner und Nudging,
ZD 2021, 404.
DSGVO

Datenschutz – aber richtig

Text: Admir Kulin

Gerade im Gesundheitswesen halten sich häufig nicht validierte Aussagen, die dem Datenschutz Todschlagargumente und die Eigenschaft des Verhinderers zusprechen. Ausssagen, die mal wieder zeigen: Es hat eben nicht Recht, wer am lautesten schreit. Vorbild-Projekte zeigen wie es geht und vereinen Informationssicherheit, Datenschutz und Digitalisierung.

Digitale Lösungen im Gesundheitswesen? „Geht nicht, Datenschutz!“ war noch vor ein paar Jahren das Todschlagargument. Mittlerweile ist klar: Das eine geht nicht ohne das andere. Wobei Datenschutz keinesfalls zum Bremsklotz für Technologie oder Digitalisierung werden muss, wie das Beispiel der Patientenportale zeigt. Denn als m.Doc 2016 mit der Vision gestartet ist, dass in Zukunft jeder Mensch jederzeit und überall seine Ärztin oder seinen Arzt „in der Tasche“ dabei hat, war eine digitale Lösung wie ein Patientenportal in einem Krankenhaus noch völlig undenkbar. Das gebe der Datenschutz nicht her, war die einstimmige Meinung.

> Digitale Lösungen im Gesundheitswesen? „Geht nicht, Datenschutz!"

Nicht einmal vier Jahre später hat die Bundesregierung mit dem Krankenhauszukunftsgesetz, kurz KHZG, den Weg für das Unmögliche geebnet. Patientenportale sind ein eigenständiger Fördertatbestand dieser Digitalisierungsinitiative für den stationären Bereich und mit 1.130 gestellten Anträgen werden sie bald flächendeckend ihren Platz in der Versorgung behaupten.

Für Dr. Silke Scholz, Chief Legal Officer bei m.Doc, war ohnehin klar, dass der Datenschutz nur vorgeschoben wurde: „Ich bin leidenschaftliche Datenschützerin und habe von Anfang an gesagt: Das ist nur ein Pseudoargument. Datenschutz muss kein Hindernis sein, sondern kann im Gegenteil zu einer wichtigen Stütze werden – beispielsweise, wenn Daten eines Patienten, die in einem Krankenhaus erhoben wurden, später in einer anderen Einrichtung (z.B. der anschließenden Reha) ebenfalls genutzt werden können. Die Herausforderung ist lediglich, es technisch so zu gestalten, dass die Patientinnen und Patienten es wissen, zustimmen und nachverfolgen können.“ Datenschutz und Technik seien demnach im Gesundheitswesen quasi die zwei Seiten ein und derselben Medaille. Digitale Lösungen sind ohne durchdachten Datenschutz nicht möglich. Gleichzeitig verbessert die uns heute zur Verfügung stehende Technik den Datenschutz ungemein.

Cloud wird sich durchsetzen

Die Datenschutz-Diskussion, die noch vor ein paar Jahren über Patientenportale geführt wurde, konzentriert sich heute auf die Cloud. On-premise sei sicherer, lautet in der Regel die Argumentation. Doch wenn man ganz genau hinschaut, funktioniert die Zukunft des Gesundheitswesens nicht ohne die Cloud. Beispiele sind die elektronische Patientenakte, die nur dann eine breite Akzeptanz erfahren kann, wenn sie Cloud-basiert und damit für die Nutzerinnen und Nutzer komfortabel ist. Und auch weitergedacht ist der Einsatz neuer Technologien wie der Künstlichen Intelligenz oder von Natural Language Processing, kurz NLP – gemeint sind Techniken und Methoden zur maschinellen Verarbeitung natürlicher Sprache – ohne entsprechende Cloud-Lösungen nicht möglich. „Wir brauchen zwingend eine agile, anpassungsfähige und skalierbare IT-Infrastruktur im Gesundheitswesen – auch mit Blick auf die Kosten. Anstatt also über die Anschaffung von Hardware zu sprechen, müssten wir über Schnittstellen und Shared Infrastructure nachdenken.

> „Wir brauchen zwingend eine agile, anpassungsfähige und skalierbare IT-Infrastruktur im Gesundheitswesen – auch mit Blick auf die Kosten.
>
> ADMIR KULIN, CEO DER M.DOC GMBH

Nur die Cloud bietet uns den Spielraum, den wir brauchen, um den dynamischen Prozess der ‚Zukunftsgestaltung' immer wieder neu zu hinterfragen, gegebenenfalls den Kurs anzupassen, nur um dann wieder Vollgas geben zu können", betont Admir Kulin, CEO der m.Doc GmbH.

Es sind also nicht ‚nur' Updates, die über die Cloud einfacher und kostengünstiger eingespielt werden können, es ist vor allem die Flexibilität, die die Neugestaltung des Gesundheitswesens dringend benötigt. Und das scheinen Argumente zu sein, die mittlerweile auch bei den Datenschützern ankommen. So hat der bayrische Landtag erst im Juni dieses Jahres die Rechtsordnung zum Outsourcing bayrischer Krankenhaus-IT liberalisiert. Damit sind nun endlich auch die dortigen Kliniken in der Lage, den digitalisierten und vernetzten Teil ihrer Patientenversorgung auf den neuesten, heutzutage meist cloudbasierten, technologischen Stand zu heben.

Privacy by Design

Auch Osiris Roost, Chief Technology Officer bei m.Doc, tendiert dazu, der Daten- und Informationssicherheit den Stellenwert einzuräumen, den sie benötigt, das Thema gleichzeitig jedoch nicht überzubewerten: „Absolute Sicherheit gibt es in keinem System. Flugzeuge sind das sicherste Transportmittel und trotzdem stürzen immer wieder welche ab. Für ein Höchstmaß an Sicherheit gibt es deshalb Standards und Richtlinien. Klar ist aus meiner Sicht, dass wir uns aktuell in sensiblen Phase der Digitalisierung befinden, weil gerade auch mit Blick auf die Akzeptanz noch zu viel auf dem Spiel steht. Andererseits können wir Digitalisierung nicht aufhalten. Daher können wir die Systeme nur so gut und so sicher konzipieren, wie möglich - und müssen kontinuierlich an Verbesserungen arbeiten."

Für das „so sicher, wie möglich" hat man bei m.Doc einen klaren Ansatz: Privacy by Design. Welche personenbezogenen Daten werden wirklich benötigt? Hier muss sich ein Anbieter wirklich Schritt für Schritt durcharbeiten – für ein Höchstmaß an Datenschutz und noch lange bevor ein Entwickler auch nur eine Zeile Code geschrieben hat. Ziel dabei ist immer, mit so wenig personenbezogenen Daten zu arbeiten, wie möglich, betont Silke Scholz: „Dafür ist es essenziell, sich in einem frühen Stadium zu fragen, was brauche ich und was brauche ich nicht. Nichts anderes ist Privacy by Design." Genau deshalb werden bei m.Doc auch keine Daten auf irgendwelchen Endgeräten geladen. Dort kommen „nur" die Informationen an. Und genau an solchen Stellen zeigt sich der große Vorteil digitaler Lösungen: Wenn jemand mit seiner Aktentasche voller Arztbriefe in eine Klinik kommt und die gestohlen wird, sind die Daten weg. War nur das Smartphone in der Aktentasche, haben die Diebe im Idealfall keinen Zugriff auf die Daten, die Patientinnen und Patienten können sie aus der Cloud jedoch wieder abrufen.

INDIVIDUELLES COACHING

„So quotieren Sie Informationssicherheit in Ihren KHZG-Förderprojekten"

bei Prof. Dr. Thomas Jäschke | Medizininformatiker und Professor für Wirtschaftsinformatik, KHZG-Experte, Vorstand der DATATREE AG

Verantwortliche in Krankenhäusern sowie Hersteller:innen sind durch die Anforderungen des Bundesamtes für Soziale Sicherung (BAS) zunehmend verunsichert: In der Empfehlung zur Umsetzung von IT- und Sicherheitsmaßnahmen im Rahmen von Fördervorhaben aus dem Krankenhausfonds sind nach §14a Abs.3 Satz 5 KHG die Anforderungen, mindestens 15 Prozent der zur Förderung gewährten Mittel für Maßnahmen zur Verbesserung der Informationssicherheit zu verwenden. In vielen Anträgen erfolgte der Nachweis von Sicherheitsmaßnahmen allerdings nicht korrekt.

Medizininformatiker Prof. Dr. Thomas Jäschke bietet Ihnen und Ihren Mitarbeitenden konkrete Umsetzungshilfen an. Der KHZG-Experte geht in einem individuell vereinbarten Termin mit Ihnen und Ihren Mitarbeitenden auf Ihre Fragen ein und bietet konkrete Umsetzungsmöglichkeiten an.

„Ich unterstütze Unternehmen bei der Einordnung der BAS-Quotierungsempfehlung zur Umsetzung der geforderten Informations- bzw. IT-Sicherheit. Dabei gebe ich auch Umsetzungsanreize in Bezug auf die bevorstehende Auswahl von Lieferant:innen und Dienstleister:innen", berichtet Thomas Jäschke, der seit über 30 Jahren als Experte im Gesundheitswesen agiert.

Die Einordnungen und Empfehlungen wurden in einem Whitepaper zusammengefasst, das Teilnehmenden am Ende des Coachings ausgehändigt wird.

BEI INTERESSE AN EINEM INDIVIDUELLEN COACHING:

Wie Sie das Coaching bei Prof. Dr. Thomas Jäschke in Anspruch nehmen können und wann Sie die Beratung kostenlos erhalten, erfahren Sie in diesem Beitrag:

TTDSG
EINE SPUREN-SUCHE

Vor kurzem hatte das Warten von uns Datenschützer:innen endlich ein Ende und wir konnten unsere Köpfe in die deutsche Umsetzung der ePrivacy-Richtlinie (RL 2002/58/EG) versenken. Eine längst überfällige Entwicklung, wenn Sie mich fragen. Das TTDSG bringt einiges an Komplexität für die praktische Umsetzung mit sich – jedoch nichts, was wir nicht gemeinsam lösen könnten.

Der Ursprung

Die deutsche Umsetzung der ePrivacy-Richtlinie hört in voller Länge auf den Namen „Telekommunikations-Telemedien-Datenschutz-Gesetz" oder kurz TTDSG. Was vielen gar nicht mehr bewusst ist: Bei unserem aktuellen TTDSG handelt es sich bereits um den zweiten Versuch einer richtlinienkonformen Umsetzung der ePrivacy-Richtlinie.

Der vorherige Anlauf in der im Jahr 2004 vom deutschen Gesetzgeber erlassenen Novellierung des Telekommunikationsgesetzes wurde nicht als ausreichende Umsetzung der Richtlinie betrachtet. Unter anderem war Art. 5 Abs. 3 der ePrivacy-Richtlinie nicht umgesetzt worden, der den Einwilligungsvorbehalt für insbesondere Cookies und andere Tracking-Technologien regelt. Hier hat der Gesetzgeber nun nachgelegt und zur Umsetzung den § 25 TTDSG geschaffen.

Diese Regelung betrifft insbesondere Cookies und andere Tracking-Technologien.

Über die Autorin Christine Thieme:
Christine Thieme ist seit 2013 bei der DATATREE AG als Beraterin im Bereich Datenschutz beschäftigt. Sie ist Expertin für Fragestellungen aus den Bereichen Beschäftigtendatenschutz, Direktmarketing und Marktforschung. Federführend setzt sie unter anderem Projekte für datenschutzkonforme Internetauftritte und E-Mail-Marketing sowie Trackingtools um.

Überschneidungen und Geltungsbereiche

Das Zusammenspiel mit benachbarten Gesetzbüchern des TTDSG bringt eine gewisse Komplexität mit sich. Inhaltlich überschneidet sich das neue Gesetz TTDSG mit dem Geltungsbereich des TKG (Telekommunikationsgesetz) und des TMG (Telemediengesetz) in ihren alten Fassungen. Jedoch ersetzt das TTDSG diese nicht. Aber was tut es dann?

Alle Normen aus den Gebieten der Telekommunikation und der Telemedien, die inhaltlich Fragen des Datenschutzes betreffen, wurden im TTDSG zusammengefasst und an die EU-Richtlinie angepasst. Alle Normen zu Fragestellungen außerhalb des Fachbereichs Datenschutz des TKG und TMG bleiben jedoch in der aktuellen Fassung bestehen und sind weiterhin gültig. So ist die Impressumspflicht für den Betreiber von Telemediendiensten - wie schon vor Inkrafttreten der Änderungen - in §5 des Telemediengesetzes verortet.

Der Schein trügt

Die praktische Umsetzung der Regelungen des TTDSG wirft jedoch in Fachkreisen noch einige Fragen auf. Insbesondere bei der Auslegung von unbestimmten Rechtsbegriffen kann bei der jungen Regelungsmaterie nicht auf eine umfassende Entscheidungspraxis der Gerichte zurückgegriffen werden. Mit der „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien" haben die deutschen Aufsichtsbehörden bereits im Dezember 2021 ihre Auslegung des neuen Gesetzes veröffentlicht.

**Klar ist jedoch folgendes:
Das TTDSG teilt sich in zwei Teile,
die verschiedene Adressaten betreffen.**

Der erste Teil beschäftigt sich mit dem „Datenschutz und dem Schutz der Privatsphäre in der Telekommunikation" und betrifft damit Anbieter:innen von Telekommunikationsdiensten und Betreiber:innen von Telekommunikationsnetzen. Für Webseitenanbieter:innen relevant ist dabei der zweite Teil, der sich mit dem Telemediendatenschutz und dem Schutz der Privatsphäre der Nutzer:innen der Endgeräte beschäftigt. Adressat dieser Normen sind nicht nur sämtliche Webseiten- und App-Betreiber:innen, sondern auch Anbieter:innen von Produkten, etwa aus dem Smart Home Bereich.

Die Praxis mit den Cookies

Des einen Freud, des anderen Leid: Was Online-Marketer vor große Herausforderungen stellt, freut die Datenschützer:innen. Das TTDSG bedeutet eine deutlich höhere Rechtssicherheit bezüglich der Frage, unter welchen Voraussetzungen der Einsatz von Trackingtechnologien in Deutschland zulässig ist. Dies ist vor allem auf das strenge Einwilligungserfordernis des § 25 TTDSG zurückzuführen. *Mehr dazu erfahren Sie in unserem Artikel „Consent-Banner: Wer blickt hier noch durch?"* auf Seite 22.

§ 25 TTDSG beschränkt sich allerdings nicht nur auf Cookies oder andere konkrete Technologien.

Der Wortlaut des Gesetzes regelt nun, das jegliche Speicherung von neuen Daten oder Informationen auf dem verwendeten Endgerät sowie der Abruf dort bereits vorhandener Informationen durch die App oder die Website der Einwilligung des Nutzenden bedürfen. Dies bedeutet im Klartext, dass die Notwendigkeit, eine Einwilligung einzuholen, nicht mehr nur auf die Verarbeitung von personenbezogenen Daten beschränkt ist, sondern grundsätzlich alle „Daten" und „Informationen" umfasst.

Dieses streng formulierte Einwilligungserfordernis betrifft neben dem klassischen Tracking durch Cookies auch Technologien wie das Auslesen von Browser-Fingerprinting, bei denen nach alter Rechtslage je nach Strenge der Auslegung ein Personenbezug der betroffenen Daten zumindest fraglich war. § 25 TTDSG stellt klar: Der/die Nutzer:in muss auf Grundlage von klaren und umfassenden Informationen die Einwilligung erklären, die den Anforderungen der EU-Verordnung 2016/679 genügen muss. Mit anderen Worten: Information und Einwilligung müssen DSGVO-konform sein.

Eine möglichst transparente Gestaltung kann also nicht nur die Einwilligungsbereitschaft der Nutzer:innen deutlich erhöhen, sondern ist auch Voraussetzung einer rechtgültigen Einwilligung.

Für die Praxis bedeutet das:
Überprüfen Sie die Umsetzung Ihres Consent-Banners und das Einwilligungsmanagement Ihres Webshops in Ihrer Kunden-App.

Aber gibt es jetzt gar keine Cookies mehr, welche auf anderen Rechtsgrundlagen als der Einwilligung i.S.d. Art. 6 Abs. 1 lit. a DSGVO basieren?
Eine relevante Ausnahme vom Einwilligungsvorbehalt gibt es: Ist die Speicherung von Daten oder der Zugriff auf bereits vorhandene Informationen unbedingt erforderlich, um einen ausdrücklich gewünschten Dienst seitens des Nutzers/der Nutzerin bereitzustellen, bedarf es keiner vorherigen Einwilligung.

In der Realität bedeutet das zum Beispiel:

Cookies zur Realisierung des Warenkorbs im Onlineshop dürfen gesetzt werden, nachdem der/die Besucher:in des Webshops den Button „Zum Warenkorb hinzufügen" anklickt. Auch ein Session-Cookie kann als technisch notwendig gewertet werden, der von dem/der Besucher:in getätigt wurde, um Sprache und Währung während des Websitebesuchs beizubehalten. Weiterhin stellt auch der Log-In zu einem Nutzerkonto den Bedarf eines technisch notwendigen Cookies dar. Allerdings gilt: Gibt es eine alternative Möglichkeit, die keinen Zugriff auf das Endgerät erfordert, ist diese umzusetzen.

Klare Maßstäbe zur Bewertung der technischen Notwendigkeit müssen sich noch herausbilden, folglich ist diese Ausnahme noch mit Vorsicht zu genießen. Es gibt also einen neuerlichen Anlass den Consent-Banner zu prüfen. Im Rahmen dieser Überprüfung sollte für alle Cookies, die nicht ohnehin auf einer Einwilligung beruhen, die Begründung der technischen Notwendigkeit dokumentiert werden. Wer besonderen Wert auf transparente Informationen für seine Nutzer:innen legt, kann diese zusätzliche Beschreibung in der Datenschutzerklärung ergänzen. Allen anderen hilft eine entsprechende Aufstellung dabei, den Überblick zu bewahren und künftig diese Bewertung zu überprüfen.

Und die Zukunft?

Auch wenn kein fester Zeitpunkt in Sicht ist: Die ePrivacy-Verordnung wird kommen – so viel steht fest.

Sie wird damit die Vorschriften des TTDSG obsolet machen, da auch diese EU-Verordnung unmittelbare Geltung in den Mitgliedsstaaten entfalten wird. Dies entbindet jedoch nicht von der Notwendigkeit, sich bis dahin mit den Fragen des TTDSG auseinanderzusetzen, auch, um auf den Erlass der Verordnung bestmöglich vorbereitet zu sein.

24. FACHTAGUNG UPDATE BDSG

Datenschutz in der Medizin

Erfolgreiche Projekte in der Praxis zeigen, wie Datenschutz, Informationstechnologie und die Forschung mit Gesundheitsdaten die Patientenversorgung revolutionieren. Sie bilden die Basis für die Gesundheitsversorgung der Zukunft.

Namhafte Experten aus der Praxis stellen während der UpdateBDSI-Tagung am 23. Februar 2023 von der Studienvertragsprüfung über die technische Umsetzung von Forschungsprojekten, bis hin zu ganzheitlichen KI-Projekten den Status Quo über den Datenschutz und der Informationssicherheit in der Gesundheitsforschung vor.

24. FACHTAGUNG **DATENSCHUTZ IN DER MEDIZIN**

am 23.02.2023 von 9.00 bis 17.00 Uhr im NH Hotel, Dortmund

Das Programm und die Möglichkeit zur Anmeldung erhalten Sie unter:

Die Veranstaltungsreihe ist eine anerkannte Fortbildung für Mediziner:innen und u.a. für Fachanwälte als Weiterbildungsmaßnahme ausgelegt.

Die Update BDSG-Tagung wird präsentiert von:

esturias Fachtagungen

DATATREE YOUR COMPLIANCE PROVIDER

Sie möchten die Exper*Site* regelmäßig kostenlos erhalten?

Dann schicken Sie eine Mail mit Ihren Kontaktdaten und dem Betreff „Exper*Site*" an Ihre Ansprechpartnerin Nina Kill, nina.kill@dr-jaeschke.ag.

Sie möchten auf dem Laufenden bleiben, wenn es um die Themen Informationssicherheit und Datenschutz geht?

Dann abonnieren Sie hier den Newsletter der DATATREE AG (QR-Code) oder unter: www.datatree.ag/blog

Vielen Dank für Ihr Interesse.

Impressum

ExperSite Ausgabe 02 2022 | **ISSN-Print** 2364-5636 | **ISSN-Internet** 2364-5644 | **Herausgeber:** DR. JÄSCHKE AG, Märkische Straße 212-218, 44141 Dortmund, T +49 231 964193-0 office@dr-jaeschke.ag | www.dr-jaeschke.ag | Sitz der Gesellschaft: Dortmund | **Registergericht:** Amtsgericht Dortmund | **Registernummer:** HRB 27509 | **Umsatzsteuer-Identifikationsnummer:** DE300625711 | **Vorstand:** Prof. Dr. Thomas Jäschke, Angelica Morina, B.A. | **Vorsitzende des Aufsichtsrates:** Dr. Anke Diehl | **Inhaltlich Verantwortlicher gemäß § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV:** Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Kill | **Design und Umsetzung:** Silvia Lorenz | **Druck:** www.onlineprinters.de **Auflage:** 5.000 | **Fotos: AdobeStock:** Seiten 22/24 © Nuthawut, Seite 25 © mast3r/sashapritchard, Seite 26 © Stock AndSu, Seite 32 © siraanamwong, Seite 34 © ipopba | **istockphoto:** Seiten 1/4-7 © Mironov Konstantin, Seite 12 © Tribalium, Seite 16 © Iemono, Seite 27 © Sam Edwards | **Interview:** Seiten 14-15, 29 © Nina Khan | JÄSCHKE GRUPPE: Seiten 17 © Marina Lutsyuk

www.linkedin.com/company/jaeschke-gruppe

www.instagram.com/jaeschke_gruppe/

Exper*Site* ist das Magazin der JÄSCHKE GRUPPE für
Digitalisierung, Informationssicherheit und Datenschutz

www.dr-jaeschke.ag