Please quote as: Schomberg, Sabrina; Dickhaut, Ernestine; Barev, Torben Jan & Janson, Andreas: Mithilfe von Privacy Nudging zu rechtsverträglichen Videokonferenztools. 2021. - Lecture Notes in Informatics (LNI) - Proceedings.

Gesellschaft für Informatik e.V. (GI) GI. (Hrsg.): INFORMATIK 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 979

Mithilfe von Privacy Nudging zu rechtsverträglichen Videokonferenztools

Sabrina Schomberg[1], Ernestine Dickhaut[2], Torben Jan Barev[3] und Andreas Janson[4]

Abstract: Die Covid-19 Pandemie hat zu enormen Veränderungen im Arbeitsalltag geführt. Videokonferenztools gewannen durch die Zusammenarbeit über Distanz an Bedeutung. In kürzester Zeit kamen in vielen Unternehmen Videokonferenztools verschiedener Hersteller zum Einsatz; der Datenschutz stand dabei in der Regel nicht an erster Stelle und es kam zu zahlreichen Datenschutzverstößen. Im Laufe der Pandemie rückte der Datenschutz mehr in den Fokus und es wurde nachgebessert. Wir wollen mit unserem Beitrag anregen Videokonferenztools nicht nur datenschutzkonform, sondern rechtsverträglich zu gestalten. Daher haben wir die Benutzeroberfläche eines Tools (Zoom) an den Stellen angepasst, an denen datenschutzsensibles Verhalten besonders kritisch ist. Wir zeigen, wie kleine Änderungen in der Benutzeroberfläche und die Integration von Privacy Nudges zu datenschutzsensiblem Verhalten führen können. Um diese sogenannten Privacy Nudges für Entwickelnde von Videokonferenztools so praktisch und zugänglich wie möglich zu machen, greifen wir auf das Konzept der Design Pattern aus der Systementwicklung zurück.

Keywords: Videokonferenztools, Privacy Nudging, Design Pattern, Rechtsverträglichkeit.

1 Einleitung

Die Covid-19 Pandemie hat in vielen Bereichen zu einem enormen Fortschritt der Digitalisierung geführt. Viele Betriebe haben sich bereits während der ersten Welle dazu entschieden einen Großteil der Mitarbeitenden von einem auf den anderen Tag ins Homeoffice zu schicken oder zumindest diese Möglichkeit zu eröffnen. Damit einhergehend wurden in kürzester Zeit neue Wege zur Zusammenarbeit und Interaktion über Distanz notwendig [BQS21] und stellten die Unternehmen vor Herausforderungen. Videokonferenztools diverser Anbieter wie beispielsweise Microsoft Teams, Jitsi und Zoom gewannen durch neue Arbeitsverhältnisse über Nacht an Bedeutung [Wa20], [AA21]. Der Videokonferenzanbieter Zoom erwirtschaftet beispielsweise allein im ersten

[1] Universität Kassel (DE), FG Öffentliches Recht, IT-Recht und Umweltrecht von Prof. Dr. Hornung, Henschelstraße 4 (K33), 34127 Kassel, sabrina.schomberg@uni-kassel.de.
[2] Universität Kassel (DE), FG Wirtschaftsinformatik von Prof. Dr. Leimeister, Pfannkuchstraße 1 (ITeG), 34121 Kassel, ernestine.dickhaut@uni-kassel.de.
[3]Universität Kassel (DE), FG Wirtschaftsinformatik von Prof. Dr. Leimeister, Pfannkuchstraße 1 (ITeG), 34121 Kassel, torben.barev@uni-kassel.de.
[4] Universität St.Gallen (CH), Institut für Wirtschaftsinformatik, Müller-Friedberg-Strasse 8 9000 St. Gallen, andreas.janson@unisg.ch.

CC BY SA

Quartal des Jahres 2021 etwa 328 Millionen US-Dollar, was eine Steigerung von 169 Prozent gegenüber dem Vorjahr bedeutet [Bo21]. Zahlen wie diese bestätigen die Relevanz und Abhängigkeit vieler Unternehmen von Anbietenden diverser Videokonferenztools.

Datenschutz war in der ad hoc Etablierung der Konferenztools oft nicht die erste Priorität. Es folgten negative Pressemeldungen und aufgedeckte Rechtsverstöße diverser Anbieter. Dadurch wurde auch der Datenschutz mehr diskutiert und es wurden Anpassungen vorgenommen. Lücken und datenschutzrechtliche Stolperfallen sind jedoch nach wie vor vorhanden [Be21], insbesondere wenn diese Tools im Rahmen der Arbeitstätigkeit genutzt werden. Die Arbeitgebenden sind jedoch auch im Homeoffice Verantwortlicher im Sinne der DSGVO [Wü20] und setzten sich der Gefahr von Bußgeldern aus, wenn sie diese Lücken nicht schließen. Prognosen zufolge werden Videokonferenzen auch nach der Pandemie langen Dienstreisen vorgezogen werden. Daher lohnt sich ein zweiter Blick auf vorhandene Videokonferenztools, die im Eiltempo auf den Markt gebracht wurden und bereits ersten rechtlichen Nachjustierungen unterlagen.

Um Videokonferenztools nachhaltig zu gestalten, nutzen wir das Konzept der Privacy Nudges, um diese Tools nicht bloß datenschutzkonform auszugestalten, sondern sogar rechtsverträglich [Ro93] zu designen. Ist das Ziel während der Systementwicklung, das Minimum rechtlicher Konformität gerade noch zu erreichen, um beispielsweise Sanktionen zu entgehen, spricht man von Rechtmäßigkeit. Liegt das Ziel jedoch darin die rechtlichen Anforderungen möglichst gut und umfassend zu erfüllen, wird dies mit Rechtsverträglichkeit bezeichnet. Das Konzept der Rechtsverträglichkeit hat das Ziel, nicht das kurzfristige Minimum, sondern das langfristige Optimum an Grundrechtsschutz zu gewährleisten [Th20]. Um Technik rechtsverträglich zu gestalten, werden dazu die relevanten Rahmenbedingungen analysiert und vorausschauend in die Systementwicklung integriert. Auf diese Weise soll die Zusammenarbeit über solche Tools für die Arbeitgebenden, und somit den datenschutzrechtlich Verantwortlichen, möglichst langfristig ohne rechtliche Bedenken unterstützt werden. Durch Nudging („Anstupsen“) sollen die Nutzenden der Videokonferenztools dazu gelenkt werden möglichst wenig Daten preiszugeben. Um diese sog. Privacy Nudges möglichst praktisch anwendbar und für Entwickelnde von Videokonferenztools verständlich zu machen, greifen wir auf das Konzept der Design Pattern aus der Systementwicklung zurück [Al17] und erstellen Design Pattern für die rechtsverträgliche Gestaltung von Videokonferenztools. Mithilfe der Design Pattern wollen wir eine Weitergabe des rechtlichen Wissens in die praktische Systementwicklung ermöglichen. Damit ist das übergeordnete Ziel dieses Beitrags, im Rahmen eines interdisziplinären Ansatzes, an der Schnittstelle von Recht und Informatik, die Umsetzung rechtsverträglicher Videokonferenztools mit Privacy Nudging zu beschreiben und dieses Wissen in Design Pattern zu kodifizieren und Entwickelnden zugänglich zu machen.

2 Theoretischer Hintergrund

2.1 Beschäftigtendatenschutz und Videokonferenztools

Das Thema „Homeoffice“ hat durch die Pandemie einen enormen Aufwind erfahren. Dabei lassen sich arbeitsrechtlich weitere Unterscheidungen treffen zwischen häuslicher und alternierender Telearbeit (im Privatbereich der Beschäftigten fest eingerichteter Bildschirmarbeitsplatz i. S. d. § 2 Abs. 7 S. 1 ArbStättV, welcher für die gesamte oder Teile der vereinbarten wöchentlichen Arbeitszeit als Ort der Erbringung der Arbeitsleistung festgelegt wurde) sowie mobiler Arbeit (ortsungebundenes Arbeiten an wechselnden Orten wie z. B. im Zug, im Café oder am Küchentisch) [Mü20], [KRP20]. In der Pandemie wurden vielfach Beschäftigte, die nur für die mobile Arbeit ausgestattet sind, mit ihren Laptops nach Hause geschickt, weswegen der Begriff Homeoffice in der Pandemie oft alle dieser drei Formen umfasst [DH20].

Für das Recht oder die Pflicht der Beschäftigten, dienstliche Tätigkeiten von zu Hause zu erledigen, bedarf es einer wirksamen Rechtsgrundlage. Da jedoch auch viele Beschäftigte in der Pandemie ein Interesse daran haben von zu Hause zu arbeiten dürfte es überwiegend zu einvernehmlichen Regelungen, die auch ad hoc oder konkludent möglich sind, gekommen sein [Su20]. Gerade bei einer plötzlichen Umstellung auf Homeoffice durch die Pandemie, waren die technischen und organisatorischen Voraussetzungen oft noch nicht gegeben, obwohl die Beschäftigten längst zu Hause vor den mühsam zusammengesuchten und im Eilverfahren bestellten Laptops oder sogar privaten Endgeräten saßen [Su20]. Die DSGVO kennt jedoch keinen Ausnahmezustand, wenngleich die Aufsichtsbehörden eine „gewisse Nachsicht“ für die Zeit der Umstellung versprachen [Ku20], [Wü20]. Mittlerweile prüfen die Datenschutzbehörden jedoch wieder ohne Nachsicht [Su20]. Und zwar auch bei der „Technikgestaltung“ von Softwareprodukten [KK21].

Auch im Homeoffice sind die Arbeitgebenden nach wie vor Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für jede Datenverarbeitung, die im Rahmen der Tätigkeit der Beschäftigten im Homeoffice ausgeführt wird [Wü20], [Su20]. Im Homeoffice gibt es sogar eine Reihe von zusätzlichen Stolperfallen des Beschäftigtendatenschutzes [VE20]. Dadurch, dass die Arbeitnehmenden von zu Hause, und somit aus ihrem Lebensmittelpunkt heraus, arbeiten, besteht ein erweitertes Risiko für die Privatheit der Beschäftigten. Betriebliche und private Sphären könnten vermischt und Aspekte der Privatheit unwillentlich mitverarbeitet werden. Die Gefahr der unfreiwilligen Preisgabe von Informationen über die Familie, Wohnungseinrichtung, Interessen durch Poster oder Bilder an der Wand besteht besonders durch Videokonferenztools ohne persönlichkeitsschützende Maßnahmen [Su20], [Wü20].

Viele Unternehmen standen vor der Herausforderung sich schnell für ein Videokonferenztool entscheiden zu müssen, damit die Beschäftigten auch über die Distanz zusammenarbeiten können. Dabei wurde vermehrt zu schon bekannten und oft

amerikanischen Anbietern wie Microsoft Teams, Skype for Business oder Zoom gegriffen, welche Anforderungen der DSGVO regelmäßig nicht erfüllten [Be21], [Su20]. Außerdem entschied der EuGH im Juli 2020, dass der Beschluss der Kommission über die Angemessenheit des EU-US-Privacy-Shields ungültig ist und somit die Übermittlung personenbezogener Daten aus der EU an einen Datenempfänger in den USA mit sofortiger Wirkung unzulässig ist [Eu20]. Dies führte sogar zu verschiedenen Varianten von Videokonferenztools, wie z. B. einer DSGVO-konformen Variante speziell für den europäischen Raum, die sich hinsichtlich der Datenspeicherung und -verarbeitung unterscheidet. So hat unter anderem Zoom im Jahr 2020 auf Kritik reagiert und beispielsweise sprachliche Korrekturen hinsichtlich der fälschlichen Verwendung des Begriffs „Ende-zu-Ende-Verschlüsselung“ durchgeführt [Ro20], [To20].

Um ein Videokonferenztool im Homeoffice DSGVO-konform einzusetzen müssen verschiede Anforderungen der DSGVO beachtet werden. Mit dem Diensteanbieter (hier Zoom), muss (je nach konkreter Ausgestaltung [PP21]) zunächst ein Auftragsverarbeitungsvertrag i. S. d. Art. 28 DSGVO geschlossen werden [St20], [Su20]. Dabei ist insbesondere ein angemessenes Datenschutzniveau bei Dienstanbietenden aus Drittländern zu gewährleisten. Seit dem Schrems-II Urteil des EuGH gibt es jedoch keinen Spielraum mehr für eine Übermittlung von Kundendaten in die USA auf Grundlage des Privacy Shield, da dieses wegen der dortigen Vorgaben zur Massenüberwachung für unzulässig erklärt wurde [Go20]. Bei der Nutzung von Videokonferenzlösungen sind darüber hinaus insb. die Anforderungen der Art. 24, 25 und 32 DSGVO einzuhalten [St20], [Wü20]. Zur Umsetzung der Vorgaben der DSGVO im Unternehmen gehört es dabei auch die Softwareprodukte so zu konfigurieren, dass diese für die konkrete Nutzung im Unternehmen alle Vorgaben einhalten [KK21].

Art. 25 DSGVO wird als Konkretisierung der Pflicht zur Umsetzung technischer und organisatorischer Maßnahmen durch den Verantwortlichen (Art. 24 DSGVO) verstanden [Ma18], [Ha18]. Adressat des Art. 25 DSGVO ist ausdrücklich nur der Verantwortliche, nicht jedoch der Hersteller von Verarbeitungstechnik. Für den Hersteller besteht daher grundsätzlich keine Pflicht zur datenschutzfreundlichen Ausgestaltung seiner Produkte. Er wird lediglich durch Erwägungsgrund 78 S. 4 dazu „ermutigt“. Aber die Verantwortlichen werden in der Regel nur solche Produkte kaufen, die den Anforderungen der DSGVO, insb. des Art. 25 DSGVO, gerecht werden, um sich nicht der Gefahr eines hohen Bußgeldes gem. Art. 83 Abs. 4 lit. a DSGVO auszusetzen. Denkbar ist insofern also eine mittelbare Wirkung, indem die Nachfrage and datenschutzfreundlicher Technologie die Hersteller zur Umsetzung eben dieser Anforderungen zwingt [Ma18]. Ebenfalls denkbar ist, dass der Arbeitgeber den Softwareentwickler im Rahmen der Mängelgewehrleistung in Haftung nehmen kann, wenn die Software nicht den datenschutzrechtlichen Vorgaben entspricht [Dü19], [Ha20]. Privacy Nudges können helfen, den weiten Anwendungsbereich von Art. 25 DSGVO mit Leben zu füllen [Sc19].

Gem. Art. 32 DSGVO müssen außerdem technische und organisatorische Maßnahmen getroffen werden, die die Sicherheit der Verarbeitung gewährleisten. Die Norm richtet

sich sowohl an den Verantwortlichen als auch an den Auftragsverarbeiter. Die Nichteinhaltung ist gem. Art. 83 Abs. 4 lit. a DSGVO ebenfalls bußgeldbewehrt und gem. Art. 82 DSGVO tragen sowohl der Verantwortliche als auch der Auftragsverarbeiter, jeder für seinen Verantwortungsbereich, ein Haftungsrisiko gegenüber den betroffenen Personen [La19]. Konkretere Angaben zu den erforderlichen Maßnahmen enthalten lediglich Art. 32 Abs. 1 lit. a-d, Abs. 4 DSGVO und Erwägungsgrund 83. Art. 32 Abs. 1 lit. a DSGVO und Erwägungsgrund 83 nennen zunächst Verschlüsselung - und Art. 32 Abs. 1 lit. a DSGVO darüber hinaus auch Pseudonymisierung - als technische Maßnahme der Risikominimierung. Auch wenn Zoom selbst als Hersteller nur dazu „ermutigt wird" (ErwG 78 S. 4 DSGVO) seine Produkte datenschutzfreundlich auszugestalten und ihn als (ggf.) Auftragsverarbeiter bzgl. der Anforderungen aus Art. 25 DSGVO eine mittelbare Verpflichtung trifft, so kann der Videokonferenzanbieter jedoch teilweise über Art. 32 DSGVO, welche eher die Bereiche IT-Sicherheit betrifft, direkt zur Rechenschaft gezogen werden. Dies erscheint jedoch auch sinnvoll, da der Verantwortliche in diesem Bereich keinerlei Möglichkeit hat durch einfaches Konfigurieren datenschutzrechtliche Lücken zu schließen. Ziel soll sein, dass ein datenschutzkonformes Homeoffice die Persönlichkeit der Beschäftigten nur so weit offenbart, wie schon deren betrieblicher Arbeitsplatz [Wü20]. Dies können Arbeitgebende maßgeblich erreichen, indem den zur Verfügung gestellten Geräten für das Homeoffice durch eine datenschutzfreundliche Technikgestaltung gem. Art. 25 und Art. 32 DSGVO „datenschutzrechtliche Scheuklappen" aufgesetzt werden [Wü20].

Die allgemeinen Anforderungen der DSGVO und die hier besonders hervorgehobenen Anforderungen der Technikgestaltung müssen eingehalten werden. Dabei können die sehr abstrakten Normen zum „Datenschutz durch Technik" für Unternehmen ein Risiko darstellen, da schwer sicher zu sagen ist, wann dem risikobasierten Ansatz der DSGVO genüge getan und ein Bußgeld sicher ausgeschlossen ist. Andererseits bieten die abstrakten Regelungen, gerade im Bereich der Technikgestaltung, aber auch Chancen. Es bleibt viel Raum für individuelle Umsetzungen und die Möglichkeit das Recht von morgen mit der Technikgestaltung von heute zu beeinflussen. Das Konzept der Rechtsverträglichkeit berücksichtigt dabei die Veränderung der Rechtsordnung in der Zukunft, am Maßstab heutiger Rechtsziele [Ro93].

2.2 Nudging

Individuen entscheiden sich oft irrational und zum eigenen Nachteil [Ac17]. Eine Möglichkeit Nutzende bei der Entscheidungsfindung in digitalen Arbeitssystemen zu unterstützen, sind sogenannte Nudges (vgl. auch [DR20]). *Thaler* und *Sunstein* definieren Nudging als unaufdringliche und die Entscheidungsfreiheit bewahrende Form der Entscheidungsbeeinflussung [TS08]. Was gewählt wird, hängt oft davon ab, wie die Entscheidungen präsentiert werden [WSV16]. Das Konzept Nudging kann demnach eine Vielzahl von Ansätzen beinhalten, um Entscheidungen zu beeinflussen. Laut *Kahnemanns* Dualprozess-Theorie nutzen Individuen zwei Denksysteme, um die Informationsfülle in der heutigen (digitalen) Welt besser zu bewerten und zielgerichtete Entscheidungen

treffen zu können. Das automatische Denksystem (System 1) repräsentiert unsere Intuitionen oder unseren unbewussten Autopiloten. Das reflektierte Denksystem (System 2) hingegen drückt sich durch unsere bewusste Planung und Kontrolle aus. Nudges können hingegen beide Denksysteme ansprechen [Ka03]. So können Nudges beispielsweise durch Aufmerksamkeitslenkungen oder Voreinstellungen, Individuen zu einem bestimmten Verhalten leiten und vorhersehbar steuern [Sc19].

Beim digitalen Nudging werden entsprechende Designelemente in der Benutzeroberfläche verwendet, um das Verhalten in digitalen Entscheidungsumgebungen zu leiten [WSV16]. Nudges verbieten hierbei keine Alternative oder verändern ökonomische Anreize einzelner Optionen [TS08]. Um als Nudge zu gelten, muss eine Intervention zudem leicht zu umgehen sein [TS08]. In der Software Zoom würden demnach alle Optionen zur Auswahl stehen. Das Individuum kann zu jeder Zeit frei entscheiden. Die Software würde jedoch die empfehlenswerte Option für das Individuum markieren oder vorauswählen. Durch diese Grundsätze sollen Nudges subtil zu Verhaltensänderungen führen und Individuen unterstützen. Nudges werden als eine freiheitsbewahrende (libertäre) Form des Paternalismus beschrieben, da versucht wird, gezielt Einfluss auf Entscheidungen von Menschen zu nehmen; den Entscheidenden allerdings nicht die Freiheit genommen wird, zu tun, was ihnen beliebt. Eine Unterform der digitalen Nudges sind hierbei die sogenannten Privacy Nudges. Privacy Nudging beschreibt eine gezielte Beeinflussung des Entscheidungsprozesses, um Menschen dazu zu bringen, dass diese „bessere“ Entscheidungen in Bezug auf deren Privatheit treffen und gleichzeitig ihre informationelle Selbstbestimmung berücksichtigen [Ac17], [SK18].

2.3 Design Pattern für die Weitergabe von rechtlichem Gestaltungswissen

Rechtliches Gestaltungswissen gewinnt in der Systementwicklung, insbesondere durch die DSGVO, immer mehr an Bedeutung. Heutzutage gehören rechtliche Anforderungen zu einem festen Bestandteil neuer Technologien. Die Allgegenwertigkeit heutiger Technologien ermöglicht die Sammlung und Verarbeitung einer großen Menge an personenbezogenen Daten, die besonders schützenswert sind. Jedoch fehlt Entwickelnden häufig rechtliches Fachwissen, um diese Anforderungen entsprechend umzusetzen. Hierbei können Design Pattern helfen, indem sie Lösungen für wiederkehrende rechtliche Gestaltungsherausforderungen bereitstellen und Entwickelnden bei der Umsetzung leiten [YSJ15], [Ro19], [Ha06].

Design Pattern haben ihren Ursprung in der Architektur, indem sie Lösungen für wiederkehrende Gestaltungsprobleme sammeln [Al77] und haben sich in den 90er Jahren ebenfalls in der Systementwicklung etabliert [Ga95]. Design Patterns bestehen aus Schablonen, in denen Informationen möglichst übersichtlich und einheitlich dargestellt werden. Neben der Bereitstellung von bewährten Lösungen, sind Design Pattern eine Möglichkeit, um komplexes Gestaltungswissen zugänglich und anwendbar zu machen [DJL21].

3 Praktische Anwendungsfälle

Um die Tauglichkeit des Privacy Nudging Konzepts aufzuzeigen, widmen wir uns im Folgenden der Gestaltung der Benutzeroberfläche von Zoom. Hierbei fokussieren wir die Stellen der Entscheidungsarchitektur, an denen ein datenschutzsensibles Verhalten besonders wichtig ist. Im Folgenden stellen wir zwei neue und angepasste Benutzeroberflächen vor, in denen digitale Privacy Nudges implementiert sind und die Nutzenden dazu angehalten werden weniger personenbezogene Daten preiszugeben.

3.1 Videovorschau mit Empfehlung der Nutzung eines virtuellen Hintergrundes

Art. 25 Abs. 2 DSGVO schreibt datenschutzfreundliche Voreinstellungen vor. Ton und Bild sollten daher bei Betreten eines Meetings standartmäßig ausgeschaltet sein, um die Beschäftigten davor zu schützen, unfreiwillige Eindrücke oder private Gespräche mit Familienmitgliedern zu teilen. Durch das bewusste Anschalten wird die Gefahr minimiert, dass die Beschäftigten zu spät bemerken, dass das Meeting bereits begonnen hat. Ein Meeting ganz ohne Bild und Ton eignet sich vor allem in kleinen Gruppen weniger, da Mimik und Gestik auch über die Distanz Nähe aufbauen und zu mehr Verständnis des Gegenübers führen können.

Doch auch mit diesem Schutz des bewussten Anschaltens kann der Konferenzhintergrund persönliche Informationen, wie z.B. Urlaubsfotos, Familienmitglieder oder individuelle Einrichtung der Beschäftigten preisgeben und sollte daher mit Bedacht gewählt werden. Bei der Einwahl in ein Zoom Meeting wird den Nutzenden in unserem angepassten Prozess daher als zusätzliche Schutzmaßnahme standardmäßig ein virtueller Hintergrund vorausgewählt (siehe Abbildung 1).

Dies kann ein neutraler Hintergrund sein, wie z.B. ein virtuelles Büro oder ein Unternehmenshintergrund, der verschiedene Markenaspekte des Unternehmens berücksichtigt. In diesem Szenario werden daher sogenannte Default Privacy Nudges genutzt, um die Privatsphäre der Nutzer zu schützen. Default Privacy Nudges beschreiben Standardeinstellungen im System. Da Nutzer in digitalen Umgebungen die Privatsphäre-Einstellungen häufig nicht ihren Bedürfnissen anpassen, bleibt die voreingestellte Option (der Status quo) übermäßig bevorzugt und meist unverändert (Status quo Bias) [Ac17]. In diesem Fall wird der neutrale virtuelle Hintergrund in Zoom eingestellt. *Hummel* und *Maedche* bewerten Defaults tendenziell als die stärksten Nudges [HM19]. Diese Defaults werden als sehr angenehm wahrgenommen [Sc20].

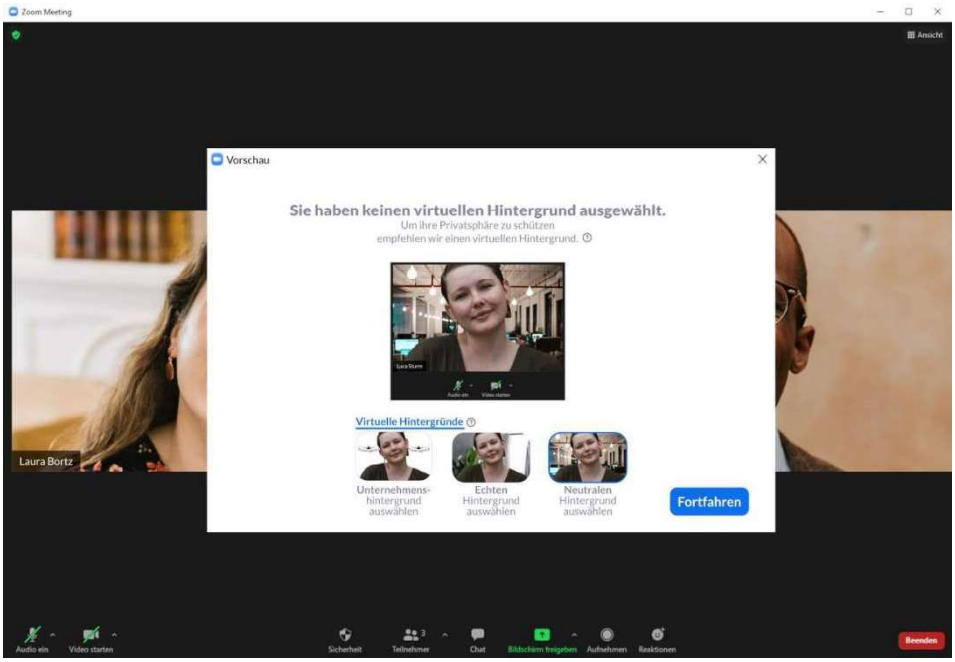


Abbildung 1. Empfehlung eines virtuellen Hintergrundes

In Bezug auf Privacy Nudging gelten Defaults als sehr effektiv, da sie in digitalen Arbeitssystemen standardmäßig das Maß der Datensparsamkeit vorgeben [Ac17]. Diese Standardeinstellungen und ähnliche leitende Maßnahmen könnten zu Reaktanz führen und dadurch eine gegenteilige Wirkung haben [BSJ21]. Reaktanz bezeichnet einen motivationalen Erregungszustand, der auftritt, wenn sich jemand in seiner Freiheit bedroht fühlt und führt zu dem Versuch die eigene Freiheit wiederherzustellen [WB75]. Einige Studienergebnisse suggerieren dies [Wa14], [Le16]. Daraus folgt die Forderung nach Transparenz. Auch für *Sunstein* gilt eine Handlung als manipulativ, wenn sie nicht transparent ist [Su15]. *Hausman* und *Welch* sind der Ansicht, dass Menschen zur Wahrung ihrer Autonomie und zum Schutz vor Missbrauch durch Nudges über solche Interventionen informiert werden sollten [HW10]. Nudges sollten demnach so gestaltet sein, dass es grundsätzlich jedem, der aufmerksam ist, möglich ist, den Nudge und die Intention der Entscheidungsarchitektur zu bemerken [Bo09]. In dem vorliegenden Szenario wurde daher ein Hinweis eingefügt, der besagt, dass die vorliegenden Einstellungen so gewählt wurden, um die Privatsphäre der Nutzer, die schützen. Außerdem fordert auch die DSGVO Transparenz (Art. 5 Abs. 1 lit. a DSGVO). Daneben gibt es auch generelle, verfassungsrechtliche Einwände gegenüber Privacy Nudges, da die informationelle Selbstbestimmung auch das Recht umfasst, möglichst viele Daten von sich selbst preiszugeben [SK18]. Eine mögliche Legitimation kann jedoch darin gesehen werden, dass die informationelle Selbstbestimmung eine Funktionsbedingung einer

demokratischen Gesellschaft und somit ein Schutzgut der Allgemeinheit ist [Sa15], [SK18]. Im arbeitsrechtlichen Kontext sind die Arbeitgebenden darüber hinaus gem. § 26 Abs. 5 BDSG zum Schutz der Daten der Beschäftigten verpflichtet [Su20].

3.2 Erweiterung der Videoaufzeichnung um pseudonyme Option

Bisher können Nutzende des Videokonferenztools Zoom der Aufzeichnung eines Meetings in der Regel nur zustimmen oder das Meeting verlassen. Die Optionen der Nutzenden könnten durch einen dritten Button erweitert werden, welcher es ermöglicht mit nur einem Klick Ton und Bild auszuschalten und den Namen zu pseudonymisieren. Im Rahmen der digitalen Arbeit wären sensible Daten nun ausschließlich für eine bestimmte Zielgruppe oder in diesem Fall, nur für das Individuum selbst zugänglich. Art. 25 Abs. 1 DSGVO nennt die Pseudonymisierung (in Art. 4 Nr. 5 DSGVO legaldefiniert), sogar als Beispiel für eine geeignete technische und organisatorische Aufgabe. Erwägungsgrund 78 führt weiterhin aus, dass der Verantwortliche interne Strategien festlegen und Maßnahmen zur Datenminimierung, schnellen Pseudonymisierung und Transparenz ergreifen soll. Der betroffenen Person soll es durch diese Maßnahmen außerdem ermöglicht werden, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche soll in die Lage versetzt werden, Sicherheitsfunktionen zu schaffen und zu verbessern. Auch wenn diese pseudonyme Option keine notwendige Anforderung nach der DSGVO ist, sie doch eine geeignete Maßnahme den Datenschutz durch Technikgestaltung umzusetzen und entspricht dem Rechtsziel. Datenschutz durch Technikgestaltung ist dabei jedoch keine einmalige Maßnahme, sondern ein stetig fortlaufender Prozess, welcher an sich wandelnde tatsächliche oder technische Gegebenheiten angepasst werden muss [La19]. Alle Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen auszuwählen und zu treffen. Dies greift unter anderem den risikobasierten Ansatz der DSGVO auf und begrenzt die Auswahl geeigneter technischer Maßnahmen [BG17], [BH17]. Dabei lässt sich mit durchdachten Benutzeroberflächen oft leicht ein bisschen mehr Datenschutz umsetzen als zwingend notwendig.

Farbelemente können die Aufmerksamkeit der Nutzenden bewusst auf die pseudonyme Option lenken und so als Privacy Nudge in die neue Benutzeroberfläche eingearbeitet werden. Die Entscheidungsalternative „Still teilnehmen“ wird durch die farbliche Hinterlegung verstärkt hervorgehoben (siehe Abbildung 2). Im aufgezeigten Szenario, wenn der Host das Zoom Meeting aufnehmen möchte, steht den Nutzern zur Auswahl, wie sie daran teilnehmen möchten. Die Vorteile der Farbelemente zeigen sich vor allem in der einfachen und kostengünstigen Umsetzung solcher Nudges, die das Individuum schnell und effektiv dazu bewegen, die eigenen Entscheidungen bezüglich des Datenschutzes und der Privatsphäre zu überdenken. Individuen können durch diese Nudges zu einem datensparsamen Verhalten geleitet werden.

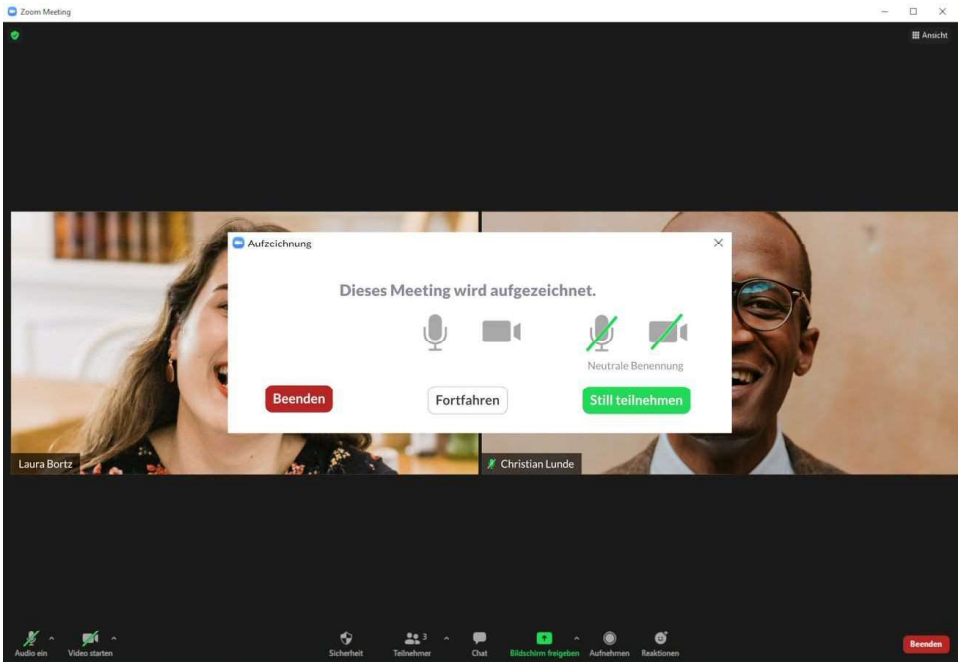


Abbildung 2. Anonyme Videoaufzeichnung

4 Erstellung von Design Pattern

Dieser Beitrag verfolgt, neben der Analyse und Empfehlung von Privacy Nudging, das Ziel dieses Wissen für die Praxis verständlich und anwendbar zu machen. In der Systementwicklung sind Design Pattern für die Kodifizierung und Weitergabe von Wissen ein bewährtes Mittel, auf welches hier zurückgegriffen wird. Die Erstellung der Design Pattern wird im Folgenden beispielhaft an dem Design Pattern „Virtueller Hintergrund“ vorgestellt, welches sich auf die Gestaltungslösungen in Abschnitt 3.1 bezieht.

Das Ziel der Design Pattern ist die Bereitstellung von Gestaltungslösungen für eine möglichst große Menge an Videokonferenztools. In Abschnitt 3 haben wir die Integration der Nudges an dem Anwendungsbeispiel Zoom veranschaulicht. Die erstellten Design Pattern können daher auch auf Zoom oder jedes weitere Konferenztool angewendet werden. Das Gestaltungswissen in den Design Pattern ist so abstrahiert, dass es keine plattformspezifischen Eigenschaften beinhaltet. Die Erstellung der Design Pattern erfolgte im Vergleich zu bekannten Methodiken der Softwareentwicklung nicht auf Basis wiedererkennbarer Muster, sondern verfolgt das Ziel bewährtes Gestaltungswissen zu kodifizieren und somit anderen Personen zugänglich zu machen.

Das Design Pattern „Virtueller Hintergrund“ (siehe Abbildung 3) stellt die Gestaltung möglicher Nudging Elemente zur Auswahl eines virtuellen Hintergrundes vor, um ungewollte private Einblicke zu vermeiden. Wie für Design Pattern üblich hat auch dieses Pattern einen eindeutigen Namen, der bereits Assoziationen mit der Gestaltungslösung auslöst. Dies ist insbesondere dann wichtig, wenn Personen sich über verschiedene Design Pattern unterhalten, und erleichtert den Austausch, indem die Intention des Patterns nicht mehr definiert werden muss. Neben dem eindeutigen Namen wird der Einsatzzeitpunkt des Nudges während der Videokonferenz dargestellt. Im Falle des virtuellen Hintergrundes setzt der Nudge an, bevor das Bild der Kamera der teilnehmenden Person für alle sichtbar ist, indem diese dazu ermuntert wird bei Einschalten der Kamera in der Videokonferenz einen virtuellen Hintergrund auszuwählen. Der Zielzustand demonstriert die bestmögliche Situation der Gestaltungslösung nach Umsetzung des Design Patterns. So sollen die Nutzenden des Videokonferenztools die Möglichkeit haben an der Konferenz teilzunehmen, ohne dabei unnötige Daten ihres privaten Umfelds preiszugeben. Die Darstellung des Gestaltungsproblems verdeutlicht die Herausforderung, der sich das Design Pattern stellt. So kann durch Teilen der Mimik und Gestik die Videokonferenz an Interaktionsmehrwert gewinnen, der jedoch ungewollte Einblicke in das private Leben geben kann. Dem Problem gegenüber steht die Lösung. Die Lösungsbeschreibung gehört zu dem wichtigsten Element im Design Pattern und gibt auf abstrakte Weise vor wie mögliche Gestaltungslösungen aussehen können.

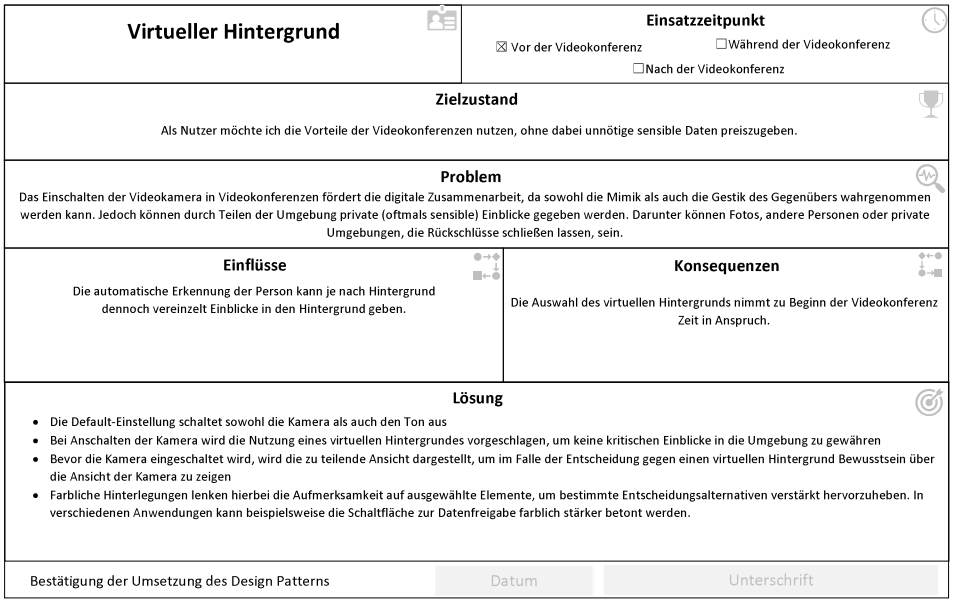


Abbildung 3: Design Pattern „Virtueller Hintergrund“

Die dargelegte Gestaltungslösung verdeutlicht, wie sie auf verschiedene Videokonferenztools generalisiert wurde und so in möglichst vielen Szenarien Unterstützung bietet. Die Integration von Nudging Elementen hängt jedoch stark von dem Kontext des Systems ab. Daher werden im Feld „Einflüsse“ Hinweise dargestellt, die vorab bei der Gestaltung und Integration der Lösung zu berücksichtigen sind. Ebenso hat die Gestaltung der vorgeschlagenen Lösung Auswirkungen auf die Funktionsweise oder Darstellung des Systems. Im Falle des Nudges zur Nutzung eines virtuellen Hintergrundes sollte daher berücksichtigt werden, dass die Auswahl des virtuellen Hintergrundes zu Beginn der Videokonferenz zu Verspätungen der Teilnehmenden führen kann. In der Systementwicklung und insbesondere dann, wenn mehrere Entwickelnde gemeinsam arbeiten ist die Dokumentation ein wichtiger Bestandteil. Daher gibt es die Möglichkeit in einem Unterschriftenfeld zu vermerken, wenn das Design Pattern implementiert wurde. So kann das Design Pattern ergänzend zu weiterer Dokumentation verwendet werden.

5 Fazit

Der vorliegende Beitrag verfolgte das Ziel, Gestaltungswissen für rechtsverträgliche Videokonferenztools unter Berücksichtigung des Privacy Nudgings zu präsentieren. Hierfür hat der Beitrag zentrale Anforderungen aus rechtlicher Sicht aufgezeigt, um den rechtlichen Rahmen abzustecken und entsprechend zu beschreiben, wie hier Rechtsverträglichkeit über die reine Konformität hinausgeht. Zudem zeigt der Beitrag auf, wie das Konzept des Nudging die rechtlichen Anforderungen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gem. Art. 25 DSGVO aus einer Gestaltungsperspektive heraus erfüllen kann und wie Design Pattern ein geeignetes Instrument zur Kodifizierung von interdisziplinärem Gestaltungswissen sein können. Kernbeitrag ist demnach die praktische Darstellung zweier Lösungen die auf den Konzepten der „Defaults“ sowie „Framing“ aufbauen, um privatheitsfreundliche und damit rechtsverträgliche Videokonferenztools zu schaffen. Die erstellten Design Pattern lassen sich auf alle gängigen Videokonferenzplattformen einsetzen und stellen somit Lösungen für wiederkehrende Probleme dar. Schließlich zeigt der Beitrag exemplarisch auf, wie sich das Gestaltungwissen für den Fall des „virtuellen Hintergrunds“ für Praxis und Forschung kodifizieren lässt. Dieses Pattern kann dabei als Startpunkt für weitere Forschung rund um die interdisziplinäre Gestaltung von Videokonferenztools dienen. Die datenschutzgerechte Gestaltung von Videokonferenztools bietet in der zunehmend digitalen Welt großes Forschungspotential. Auf Basis der dargestellten Überlegungen sollten Nutzerstudien durchgeführt werden, die zum einen die Wirkungen der integrierten Privacy Nudges auf den Nutzenden sowie deren Verhalten untersuchen.

Danksagung

Dieser Artikel wurde im Rahmen des Projekts „Nudger“ (www.nudger.de; Förderkennzeichen: 16KIS0890K; 16KIS0891) unter der Projektträgerschaft des VDI/VDE-IT erarbeitet und mit den Mitteln des Bundesministeriums für Bildung und Forschung gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

6 Literaturverzeichnis

[AA21] Anthony Jnr, B.; Abbas Petersen, S.: Examining the digitalisation of virtual enterprises amidst the COVID-19 pandemic: a systematic and meta-analysis. Enterprise Information Systems 5/15, S. 617–650, 2021.

[Ac17] Acquisti, A. et al.: Nudges for Privacy and Security. ACM Computing Surveys 3/50, S. 1–41, 2017.

[Al17] Alexander, C. et al.: A pattern language. Towns, buildings, construction. Oxford Univ. Press, New York, NY, 2017.

[Al77] Alexander, C. et al.: A pattern language. Towns, buildings, construction. Oxford University Press, New York, 1977.

[Be21] Berliner Beauftragte für Datenschutz und Informationsfreiheit: Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, 2021.

[BG17] Baumgartner, U.; Gausling, T.: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Was Unternehmen jetzt nach der DS-GVO beachten müssen. ZD, S. 308–313, 2017.

[BH17] Bieker, F.; Hansen, M.: Datenschutz "by Design" und "by Default" nach der neuen europäischen Datenschutz-Grundverordnung. RDV 4, S. 165–170, 2017.

[Bo09] Bovens, L.: The Ethics of Nudge. In (Grüne-Yanoff, T.; Hansson, S. O. Hrsg.): Preference change: Approaches from philosophy, economics and psychology. Springer Science & Business Media, S. 207–220, 2009.

[Bo21] Bocksch, R.: Zoom Video Communications. Zooms rapider Umsatzanstieg. https://de.statista.com/infografik/21927/umsatzentwicklung-von-zoom/, Stand: 07.07.2021.

[BQS21] Bai, C.; Quayson, M.; Sarkis, J.: COVID-19 pandemic digitization lessons for sustainable development of micro-and small- enterprises. Sustainable Production and Consumption 27, S. 1989–2001, 2021.

[BSJ21] Barev, T.; Schwede, M.; Janson, A.: The Dark Side of Privacy Nudging – An Experimental Study in the Context of a Digital Work Environment. In (Bui, T. Hrsg.): Proceedings of the 54th Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences, 2021.

[DH20] Dehmel, E.; Hartmann, N.: Das Coronavirus (COVID-19) auf dem Vormarsch. Die wichtigsten arbeitsrechtlichen Themen. BB (Betriebs-Berater), S. 885–891, 2020.

[DJL21] Dickhaut, E.; Janson, A.; Leimeister, J. M.: Codifying Interdisciplinary Design Knowledge Through Patterns – The Case of Smart Personal Assistants. In (Hofmann, S.; Müller, O.; Rossi, M. Hrsg.): Extending the Boundaries of Design Science Theory and Practice. 15th. SPRINGER NATURE, [S.l.], S. 114–125, 2021.

[DR20] Dominique Machuletz; Rainer Böhme: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. undefined, 2020.

[Dü19] Dümeland, M.: Sachmangelhaftigkeit von Software bei nicht DSGVO-konformer Entwicklung. Kommunikation & Recht (K&R) 1, S. 22–25, 2019.

[Eu20] EuGH: Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems. Vorabentscheidungsersuchen des High Court (Irland), 2020.

[Ga95] Gamma, E.: Design patterns: elements of reusable object-oriented software. Pearson Education India, 1995.

[Go20] Golland, A.: Datenschutzrechtliche Anforderungen an internationale Datentransfers. NJW, S. 2593–2596, 2020.

[Ha06] Hafiz, M.: A collection of privacy design patterns. In (Yoder, J. Hrsg.): Proceedings of the 2006 conference on Pattern languages of programs. ACM, New York, NY, S. 1, 2006.

[Ha18] Hartung, J.: Art. 25. In (Kühling, J.; Buchner, B. Hrsg.): Datenschutz-Grundverordnung/BDSG. Kommentar. C.H. Beck, München, 2018.

[Ha20] Hartung, J.: Art. 25: Datenschutz-Grundverordnung BDSG. Kommentar. C.H.Beck, München, 2020.

[HM19] Hummel, D.; Maedche, A.: How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies. Journal of Behavioral and Experimental Economics 80, S. 47–58, 2019.

[HW10] Hausman, D. M.; Welch, B.: Debate: To Nudge or Not to Nudge*. Journal of Political Philosophy 1/18, S. 123–136, 2010.

[Ka03] Kahneman, D.: Maps of Bounded Rationality: Psychology for Behavioral Economics. American Economic Review 5/93, S. 1449–1475, 2003.

[KK21] Klingbeil, T.; Kohm, S.: Datenschutzfreundliche Technikgestaltung und ihre vertraglichen Implikationen. Praxisnahe Anforderungen für Softwareprodukte. MMR, S. 3–8, 2021.

[KRP20] Krieger, S.; Rudnik, T.; Povedano, A.: Homeoffice und Mobile Office in der Corona-Krise. NZA, S. 473–479, 2020.

[Ku20] Kugelmann, D.: Gesundheitsnot kennt Datenschutzgebot. Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung, VerfBlog, 2020.

[La19] Laue, P.: § 7. Technischer und organisatorischer Datenschutz. In (Laue, P.; Kremer, S. Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis. Nomos, Baden-Baden, 2019.

[Le16] Lehmann, B. A. et al.: Changing the default to promote influenza vaccination among health care workers. Vaccine 11/34, S. 1389–1392, 2016.

[Ma18] Martini, M.: Art. 25. In (Paal, B. P.; Pauly, D. A. Hrsg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. C.H. Beck, München, 2018.

[Mü20] Müller, S.: Homeoffice in der arbeitsrechtlichen Praxis. Rechtshandbuch für die Arbeit 4.0. Nomos, Baden-Baden, 2020.

[PP21] Paal, B. P.; Pauly, D. A.: Einleitung: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. C.H. Beck, München, 2021.

[Ro19] Rossi, A. et al.: Legal Design Patterns: Towards A New Language for Legal Information Design. 22nd International Legal Infomatics Symposium IRIS 2019, 2019.

[Ro20] Roßnagel, A.: Zoom und Datenschutz. file:///C:/Users/Admin/AppData/Local/Temp/Zoom_und__Datenschutz_CIO_AR_23032020-1.pdf, Stand: 07.07.2021.

[Ro93] Roßnagel, A.: Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin. Zugl.: Heidelberg, Univ., Habil.-Schr., 1992. Nomos-Verl.-Ges, Baden-Baden, 1993.

[Sa15] Sandfuchs, B.: Privatheit wider Willen? Dissertation, 2015.

[Sc19] Schomberg, S. et al.: Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging. Datenschutz und Datensicherheit - DuD 12/43, S. 774–780, 2019.

[Sc20] Schöbel, S. et al.: Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach. In (Bui, T. Hrsg.): Proceedings of the 53rd Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences, 2020.

[SK18] Sandfuchs, B.; Kapsner, A.: Privacy Nudges: Conceptual and Constitutional Problems. In (Bürk, S. et al. Hrsg.): Privatheit in der digitalen Gesellschaft. Duncker & Humblot, Berlin, S. 319–338, 2018.

[St20] Stocklas, J.: Datenschutz in Zeiten von Corona. ZD-Aktuell, 2020.

[Su15] Sunstein, C. R.: Do People Like Nudges? SSRN Electronic Journal, 2015.

[Su20] Suwelack, F.: Datenschutzrechtliche Vorgaben für Homeoffice und Remote Work. Nachhaltige und rechtssichere Umstellung - New Work. New Normal. New Problems? ZD, S. 561–566, 2020.

[Th20] Thies, L. F. et al.: Konfliktäre Anforderungen an smarte persönliche Assistenten. Datenschutz und Datensicherheit - DuD 9/44, S. 573–578, 2020.

[To20] Townsend, K.: Zoom's Security and Privacy Woes Violated GDPR, Expert Says. Zoom Security Risks, Privacy and GDPR Compliance. https://www.securityweek.com/zooms-security-and-privacy-woes-violated-gdpr-expert-says, Stand: 07.07.2021.

[TS08] Thaler, R. H.; Sunstein, C. R.: Nudge. Improving decisions about health, wealth, and happiness. Yale University Press, New Haven, 2008.

[VE20] Verheyen, J.; Elgert, D.: Datenschutz im Homeoffice - Ein Überblick. K&R, S. 476–479, 2020.

[Wa14] Wang, Y. et al.: A field trial of privacy nudges for facebook. In (Jones, M. et al. Hrsg.): Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14. ACM Press, New York, New York, USA, S. 2367–2376, 2014.

[Wa20] Waizenegger, L. et al.: An affordance perspective of team collaboration and enforced working from home during COVID-19. European Journal of Information Systems 4/29, S. 429–442, 2020.

[WB75] Wortman, C. B.; Brehm, J. W.: Responses to Uncontrollable Outcomes: An Integration of Reactance Theory and the Learned Helplessness Model. Advances in Experimental Socal Psychology 8, S. 277–336, 1975.

[WSV16] Weinmann, M.; Schneider, C.; Vom Brocke, J.: Digital Nudging. Business & Information Systems Engineering 6/58, S. 433–436, 2016.

[Wü20] Wünschelbaum, M.: COVID-19: Pandemiebwältigung und Datenschutz. Kollektivvereinbarungen als krisentaugliches DS-GVO-Instrument? NZA, S. 612–616, 2020.

[YSJ15] Yskout, K.; Scandariato, R.; Joosen, W.: Do Security Patterns Really Help Designers?: Second ACM International Conference on Mobile Software Engineering and Systems - MOBILESoft 2015. May 16-17, 2015, Florence, Italy. IEEE, Piscataway, NJ, S. 292–302, 2015.