



Handlungsbroschüre Systematisches Design digitaler Privacy Nudges

Handlungsempfehlungen zur Gestaltung
von digitalen Privacy Nudges

ITeG Technical Reports

Band 12

Herausgegeben vom
Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der
Universität Kassel



Universität Kassel
ITeG Wissenschaftliches Zentrum für
Informationstechnik-Gestaltung
Pfannkuchstr. 1
D-34121 Kassel

Handlungsbroschüre

Systematisches Design digitaler Privacy Nudges

Handlungsempfehlungen zur Gestaltung von digitalen Privacy Nudges

Autoren*

Torben Jan Barev

Ernestine Dickhaut

Sabrina Schomberg

Dr. Andreas Janson

Dr. Sofia Schöbel

Dr. Thomas Grote

Prof. Dr. Gerrit Hornung

Prof. Dr. Jan Marco Leimeister

* Die Reihenfolge der ersten drei Autoren ist alphabetisch.
Die ersten drei Autoren haben zu gleichen Teilen beigetragen.

Fachgebiet Wirtschaftsinformatik
Prof. Dr. Jan Marco Leimeister
Universität Kassel/ Wissenschaftliches Zentrum für IT-Gestaltung
(ITeG) Pfannkuchstraße 1
34121 Kassel

Fachgebiet Öffentliches Recht, IT-Recht & Umweltrecht
Prof. Dr. Gerrit Hornung
Institut für Wirtschaftsrecht (IWR)
Henschelstraße 4
34127 Kassel

Gestaltung, Koordination & Redaktion:

Sabrina Schomberg
Ernestine Dickhaut
Torben Jan Barev
Lena Hortsch

Projekt:

Diese Broschüre ist im Rahmen des BMBF-Projektes „Nudging Privacy in der digitalisierten Arbeitswelt – Systematische Konzeptentwicklung und Pilotierung (Nudger)“ entstanden. Das Projekt wurde mit den Mitteln des Bundesministeriums für Bildung und Forschung gefördert (Förderkennzeichen: 16KIS0890K; 16KIS0891). Die Laufzeit des Projektes war vom 01.09.2018 bis 31.12.2021.



Diese Veröffentlichung – ausgenommen Zitate und anderweitig gekennzeichnete Teile – ist unter der Creative-Commons-Lizenz Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0: <https://creativecommons.org/licenses/by-sa/4.0/deed.de>) lizenziert.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

ISBN 978-3-7376-1088-9

DOI: <https://doi.org/10.17170/kobra-202210287049>

© 2022, kassel university press, Kassel
<https://kup.uni-kassel.de>

Vorwort

Liebe Leserinnen und Leser,

dies ist der zwölfte Beitrag, der im Rahmen der Serie „ITeG Technical Reports“ erscheint. Das Wissenschaftliche Zentrum für Informationstechnik-Gestaltung (ITeG) ist eine Forschungseinrichtung der Universität Kassel. Es widmet sich der interdisziplinären Gestaltung gesellschaftlich wünschenswerter Informations- und Kommunikationstechnik aus einer soziotechnischen Perspektive. Mit der Bündelung von Kompetenzen aus Informatik, Ergonomie, Technikrecht, Wirtschaftsinformatik, Soziologie, Gender- und Diversityforschung sowie Wirtschaftspsychologie ist das ITeG ein auf die nachhaltige Stärkung des Forschungsprofils der Universität Kassel ausgerichteter Forschungsverbund.

Ein an den Fachgebieten Wirtschaftsinformatik und Öffentliches Recht, IT-Recht & Umweltrecht angesiedeltes Projekt war das durch das Bundesministerium für Bildung und Forschung geförderte Projekt „Nudging Privacy in der digitalisierten Arbeitswelt – Systematische Konzeptentwicklung und Pilotierung“ (Nudger). Das Verbundprojekt Nudger entwickelte innovative Konzepte und zugehörige IT-Systeme für die digitale Arbeitswelt der Zukunft unter der Berücksichtigung von sogenannten Nudges zur Sicherstellung von Privatheit und informationeller Selbstbestimmung. Das Nudging („Anstupsen“) hat seinen Ursprung in der Verhaltensökonomik. Es zielt darauf ab, das Verhalten von Nutzenden vorhersehbar zu beeinflussen, ohne Anweisungen und Verbote auszusprechen. Im Rahmen des Projektes wurde untersucht, inwiefern der Einsatz von Nudges in der digitalen Arbeitswelt zur Sicherung von Privatheit und informationeller Selbstbestimmung beitragen kann. Im Rahmen des Projektes wurde ein Vorgehen entwickelt, welches zugleich juristische und ethische Randbedingungen benennt, um digitale Nudges systematisch zu entwickeln. Anbietende von digitalen Arbeitssystemen können die Ergebnisse des Projektes verwenden, um Privatheit und informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Daten zu unterstützen. Dies wird auch in Hinblick auf die Vorgaben der Datenschutz-Grundverordnung entscheidend dazu beitragen, die Marktakzeptanz solcher Lösungen maßgeblich zu steigern.

Zusätzlich zu den entwickelten Designtools wurde diese Handlungsbroschüre für die Entwicklung von digitalen Nudges bereitgestellt, die für zahlreiche andere Projekte der Technikgestaltung und -entwicklung genutzt werden kann. Damit baut dieser Band auf den ersten Ausgaben der Technical Reports des ITeG auf, die sich bereits mit der Gestaltung von Software und digitalen Systemen beschäftigt haben. Bereits im Technical Report 2 wurden Entwurfsmuster, im Technical Report 3 Anforderungsmuster zur Unterstützung der Entwicklung von Informationssystemen eingesetzt. Das Projekt stellt einen wichtigen Beitrag dar, indem es untersuchte, inwiefern der Einsatz von Nudges in der digitalen Arbeitswelt zur Sicherung von Privatheit und informationeller Selbstbestimmung beitragen kann. Dabei betrachtete das Projekt diese Fragestellung interdisziplinär aus einer technischen sowie einer gesellschaftswissenschaftlichen Perspektive und berücksichtigte gleichermaßen juristische und ethische Aspekte.

Die in dieser Handlungsbroschüre dargelegten Erkenntnisse beruhen auf Publikationen, die sich mit dem Thema Nudging befassen und von den Autoren bereits publiziert wurden. Eine Übersicht über die publizierten Beiträge finden Sie im Publikationsverzeichnis.

Eine anregende und informative Lektüre wünschen Ihnen

Prof. Dr. Jan Marco Leimeister

Prof. Dr. Gerrit Hornung

Inhalt

Vorwort	vii
Abbildungsverzeichnis	3
Tabellenverzeichnis	4
1 Einführung	5
2 Begriffliche Grundlagen	7
2.1 Nudging	7
2.2 Digitales Nudging	7
2.3 Hypernudging	8
2.4 Entscheidungsarchitektur	8
2.4.1 Duale Prozesstheorie	8
2.4.2 Privatsphäre Paradox: Präferenzen und Privatheit	9
2.5 Digitale Arbeitssysteme	10
2.6 Datenschutz	10
3 Privacy Nudging im digitalen Kontext	12
3.1 Charakterisierung von Privacy Nudges	12
3.2 Prinzipien des Privacy Nudgings	13
3.2.1 Rechtliche Rahmenbedingungen (DSGVO)	13
3.2.2 Besonderheiten digitaler Privacy Nudges	14
3.2.3 Privacy Nudges im digitalen Arbeitskontext	15
4 Systematisches Design von digitalen Privacy Nudges	18
4.1 Anforderungen an das Design und die Implementierung	18
4.2 Design Prinzipien für digitale Privacy Nudges	19
5 Kodifizierung des Gestaltungswissens	20
5.1.1 Entwicklung von Nudge Entwurfsmustern	20
5.1.2 Entwurfsmuster für die Gestaltung datenschutzgerechter Videokonferenzsysteme	22
6 Das DELEN Modell	24
6.1 Designprozess	24
6.2 Implementierungsprozess	25
6.3 Überarbeitungs- und Optimierungsprozesse	26
7 Anwendung	27
8 Evaluation	29
8.1 Intention	29
8.2 Mechanismen	29
8.3 Ethische Bewertung	30

8.4	Rechtswissenschaft	31
9	Empfehlungen	34
10	Fazit	35
11	Literaturverzeichnis.....	36
	Publikationsverzeichnis der im Projekt erarbeiteten Forschungspapiere	41

Abbildungsverzeichnis

Abbildung 1: Eigene Darstellung. Entwurfsmuster „Color Framing Nudge“	21
Abbildung 2: Eigene Darstellung. Entwurfsmuster „Virtueller Hintergrund“	22
Abbildung 3: Eigene Darstellung. DELEN Prozessmodel	24
Abbildung 4: Eigene Darstellung. Anwendungsszenario	28

Tabellenverzeichnis

Tabelle 1: Design Anforderungen..... 18

Tabelle 2: Design Prinzipien 19

1 Einführung

Die Digitalisierung verändert unsere Gesellschaft, die Art wie wir miteinander kommunizieren und wie wir arbeiten. Diesbezüglich birgt die Digitalisierung nicht nur Vorteile, sondern führt auch dazu, dass jedes Individuum durch sein Agieren in der digitalen Welt Datenspuren hinterlässt. Diese Daten werden gesammelt, aggregiert und ausgewertet, und das vielfach, ohne dass sich Individuen dessen bewusst sind (Belanger and Hiller 2006). Dementsprechend ergeben sich nicht nur für Individuen Risiken, sondern auch für Unternehmen, deren Angestellte durch ihre Arbeit Daten preisgeben und teilen. Für Individuen wird es vermehrt schwieriger, zu entscheiden und zu erkennen, welche Daten sie gefahrlos mit anderen teilen können.

Es bedarf somit innovativer Lösungen, die sowohl die Chancen der Digitalisierung ausschöpfen als auch gleichzeitig gewährleisten, dass seitens der Individuen sorgsam mit Daten umgegangen wird. Um beides zu fördern, kann das sogenannte Privacy Nudging wertvolle Unterstützung bieten, welches das Verhalten in digitalen Umgebungen vorhersehbar dahingehend beeinflussen soll, dass datenschutzfreundliche Entscheidungen durch Individuen getroffen werden (Acquisti et al. 2017; Weinmann et al. 2016). Ein Nudge dient dazu, Individuen gewissermaßen „anzustupsen“, um sie durch den Einsatz von Steuerungselementen und ohne jegliche Einschränkung dazu zu bewegen, ihr Verhalten zu ändern (Thaler and Sunstein 2008b). Das Konzept des Privacy Nudgings ist besonders relevant, da Individuen sich oftmals gar nicht darüber bewusst sind, in welcher Form die von ihnen preisgegebenen Daten verarbeitet und durch andere weiter genutzt werden. Das Konzept des Privacy Nudgings hat sich bereits in vielen Kontexten als sinnvoll und effektiv erwiesen. Es kann beispielsweise eingesetzt werden, um Nutzende vor versehentlicher Datenpreisgabe zu schützen (Schomberg et al. 2019) oder sie dazu bewegen sorgsamer in sozialen Medien zu agieren (Eigenbrod and Janson 2018).

Digitale Arbeitsumgebungen sind heutzutage allgegenwärtig. Zugleich hat die Anzahl an Möglichkeiten, Informationen über Arbeitstätigkeiten sowie sensible persönliche Daten elektronisch zu erfassen, drastisch zugenommen (Backhaus 2019). Unternehmen nutzen immer mehr Formen von digitalen Arbeitssystemen und setzen fortschrittliche Instrumente wie Big Data Analytik oder Künstliche Intelligenz ein. Damit können Daten schneller und in größerem Umfang als je zuvor gesammelt, aggregiert und analysiert werden (Malhotra et al. 2004). Darüber hinaus können Daten gesammelt werden, ohne dass der Einzelne davon weiß (Bélanger and Crossler 2011). Auf der einen Seite birgt die weit verbreitete Analyse von persönlichen Daten ein erhebliches Innovationspotenzial, einen wirtschaftlichen Wert sowie effizientere Arbeitsmodelle (Erevelles et al. 2016). Auf der anderen Seite ist die Anfälligkeit für Diskriminierung, kommerzielle Ausbeutung und unerwünschte Überwachung ebenso allgegenwärtig. Dadurch wird die Akzeptanz moderner IT-Systeme behindert. Dieser Interessenkonflikt wird sich in den kommenden Jahren vermutlich noch verschärfen, da die Unternehmen von der fortschreitenden Digitalisierung profitieren.

Das Problem besteht darin, dass die Menschen ihre Privatsphäre schätzen, sie aber nicht immer schützen; dieses Phänomen ist als „Privacy Paradox“ bekannt (Barth and Jong 2017). Da die Privatsphäre eine kritische Voraussetzung für die Akzeptanz zukünftiger Arbeitssysteme ist, werden innovative Lösungen für Informationssysteme benötigt, die Risiken für die Privatsphäre mindern und den Schutz von Informationen fördern. Eine mögliche Lösung wären Privacy-by-Design-Systeme, die datenschutzfördernde Technologiekomponenten sind (Spiekermann 2016).

Ein Mechanismus, um dies zu erreichen, ist die Einführung von „Privacy Nudges“. Nudges werden beschrieben als „jeder Aspekt der Entscheidungsarchitektur, der das Verhalten der Menschen auf

vorhersehbare Weise verändert, ohne Optionen zu verbieten, oder ihre wirtschaftlichen Anreize wesentlich zu verändern“ (Thaler and Sunstein 2008b). Daher sollten Nudges zum Schutz der Privatsphäre den Nutzenden helfen, bessere Datenschutzentscheidungen zu treffen (Acquisti et al. 2017). Ihre Wirksamkeit ist jedoch unterschiedlich (Sunstein 2015). Es stellt sich heraus, dass einige Nudges nur geringe oder gar keine Auswirkungen auf das tatsächliche Verhalten haben (Sunstein 2017). Somit wurden im Rahmen des Projektes verschiedene Gestaltungsprinzipien abgeleitet.

2 Begriffliche Grundlagen

Die für das Forschungsprojekt Nudger wichtigsten Ansätze des Nudgings und insbesondere des digitalen Nudgings sowie die dazugehörigen Begrifflichkeiten der Entscheidungsarchitektur und des Datenschutzes werden im Folgenden kurz erläutert.

2.1 Nudging

Nudging gibt es sowohl im realen als auch im digitalen Bereich. Nudging kann eine Vielzahl von Ansätzen zur Beeinflussung von Entscheidungen beinhalten. Was gewählt wird, hängt oft von der Art und Weise ab, wie die Entscheidungen präsentiert werden (Weinmann et al. 2016). Nudging basiert auf dem Prinzip des libertären Paternalismus, um Entscheidungen zu beeinflussen. Dies bedeutet, dass ein Individuum jederzeit eine Entscheidungsoption frei wählen kann (Liberalismus-Komponente). Die Wahlfreiheit des Einzelnen wird nicht eingeschränkt, da keine der Optionen verboten ist und der wirtschaftliche Anreiz der Alternativen nicht wesentlich verändert wird. Allerdings wird das Individuum zu einer Entscheidungsoption gedrängt, die den vermeintlich größten Nutzen für es darstellt (Paternalismus-Komponente) (Thaler and Sunstein 2008b).

Der Ansatz des sanften oder libertären Paternalismus ist dabei die Grundlage des Nudgings. Somit werden Nudges dazu genutzt, Individuen zu Entscheidungen zu bewegen, die für die Gesellschaft vorteilhaft sind, aber auch im langfristigen Interesse des Einzelnen liegen, ohne ihm die Wahl zwischen möglichen Optionen und Entscheidungen zu nehmen.

2.2 Digitales Nudging

Beim digitalen Nudging wird dieses Konzept auf den digitalen Raum übertragen und es werden entsprechende Designelemente in der Benutzeroberfläche zur Steuerung des Verhaltens in digitalen Entscheidungsumgebungen eingesetzt. Digitale Entscheidungsumgebungen sind Benutzeroberflächen, die von Menschen Urteile oder Entscheidungen verlangen, wie zum Beispiel Kaufentscheidungen in einem digitalen Geschäft. Im Bereich der Sicherheit und des Schutzes der Privatsphäre ist der Grundgedanke hinter der Verwendung von Nudges, den Menschen Anstöße für wohlüberlegte und informierte Entscheidungen zum Schutz der Privatsphäre zugeben. Bei diesen Nudges geht es darum, die informationelle Selbstbestimmung des Einzelnen zu bewahren und sie zu befähigen, Entscheidungen zu treffen, die ihre Datensicherheit und Privatsphäre wirksam schützen.

Die Gestaltung von digitalen Nudges hat demnach zum Ziel, Nutzende zu ihrem Vorteil in eine bestimmte Richtung zu „stupsen“ und zwar durch den Einsatz von Elementen, wie beispielsweise dem farblichen Hervorheben von datenschutzfreundlichen Optionen, welches durch das sogenannte Framing vorgenommen werden kann. Nudges können dabei nicht nur in realen Umgebungen (wie durch den Einsatz einer Lebensmittelampel), sondern auch im digitalen Raum (in Form von Voreinstellungen) verwendet werden. Nudges kommen vor allem dann zum Einsatz, wenn viele Entscheidungsalternativen verfügbar sind oder die Entscheidung sehr komplex ist (Hummel and Maedche 2019). Digitale Nudges sind speziell für das Web entwickelt worden. *Weinmann et al.* definieren digitale Nudges als Anwendung von Elementen für Benutzeroberflächen, um Wahlmöglichkeiten von Nutzenden in digitalen Umgebungen zu unterstützen (Weinmann et al. 2016).

Meske and Potthoff erweitern diese Definition um die Aspekte der freien Entscheidung sowie der Nutzung von Informations- und Interaktionselementen (Meske and Potthoff 2017). Interaktionselemente oder allgemein und fortan Nudge Elemente genannt können unterschiedlich ausgeprägt sein.

Digitale Entscheidungsumgebungen sind Benutzeroberflächen, die von Menschen verlangen, Urteile oder Entscheidungen zu treffen. Wie in Offline-Umgebungen gibt es auch in Online-Umgebungen keine neutrale Möglichkeit, Wahlmöglichkeiten zu präsentieren. Jede Benutzeroberfläche, von Unternehmenswebsites bis hin zu mobilen Apps, kann daher als digitale Entscheidungsumgebung betrachtet werden (Weinmann et al. 2016).

2.3 Hypernudging

Der digitale Bereich ist für den Nudging-Diskurs in zweifacher Hinsicht relevant. Erstens sind digitale Technologien ein Mittel, um Nudges hervorzubringen. Zweitens sind digitale Technologien die Grundlage für Entscheidungsarchitekturen, welche durch Nudges auf moralisch zulässige oder unzulässige Weise manipuliert werden. Digitale Technologien ermöglichen es, Nudges auf das Persönlichkeitsprofil einzelner Personen zuzuschneiden. Hierbei ist die Rede von Hypernudges (Yeung 2017). Diese sind aus ethischer Sicht jedoch als höchst problematisch anzusehen, insbesondere da sie mit den Bedingungen für psychologische Autonomie in Konflikt stehen. Durch die Personalisierung kann es zu schwer werden, Nudges zu widerstehen, womit nicht mehr sinnvollerweise Handlungsfreiheit angenommen werden kann. Wenn die Entscheidungsarchitektur bei digitalen Technologien manipuliert wird, stellt sich wiederum die Frage, wie sich Transparenz gewährleisten lässt. Dies ist insbesondere bei opaken KI-basierten Systemen der Fall.

2.4 Entscheidungsarchitektur

2.4.1 Duale Prozesstheorie

Im täglichen Leben haben die Nutzenden selten genügend Zeit und Informationen, um alle Alternativen vollständig zu bewerten. Anstatt eine systematische Entscheidungsfindung zu betreiben, greifen die Nutzenden auf sogenannte Heuristiken (mentale Abkürzungen) zurück (Hertwig and Grüne-Yanoff 2017). Heuristiken sind informelle Faustregeln, die die Komplexität von Entscheidungen reduzieren und somit Abkürzungen in der Entscheidungsfindung darstellen. Heuristiken sind zwar eine effiziente Hilfe, um wiederkehrende Probleme zu lösen, jedoch können sie somit auch zu systematischen Fehlern führen, wie beispielsweise Verzerrungen bei der Informationsbewertung (Tversky and Kahneman 1974).

Um zu zeigen, warum Personen Informationen preisgeben, wird der allgemeine Entscheidungsprozess vorgestellt. Dieser beginnt mit einer Situation, die eine Entscheidung oder ein Verhalten erfordert. Jedes Individuum bewertet diese Situation zunächst kognitiv. In diesem Prozess bilden sich die Individuen Meinungen, ziehen Schlussfolgerungen und bewerten Ereignisse oder Personen kritisch. Je nachdem, wie die Individuen eine Situation kognitiv bewerten, löst sie unterschiedliche Emotionen aus (positiv, negativ oder neutral). Sowohl die kognitive Bewertung als auch die Gefühle können die Entscheidung dann beeinflussen.

Entscheidungen werden somit häufig nicht auf Basis von rationalen Überlegungen getroffen, sondern auf Basis von Heuristiken, welche den Entscheidungsprozess systematisieren (Mongin and Cozic 2018). Ein Erklärungsansatz dafür ist die duale Prozesstheorie von *Kahneman*, die besagt, dass Individuen zwei Denksysteme benutzen. Zwei Systeme sind notwendig, um die Informationsfülle in der heutigen (digitalen) Welt besser einschätzen und gezielte Entscheidungen treffen zu können. System 1 repräsentiert Intuitionen wie ein unbewusster Autopilot. System 2 hingegen äußert sich durch eine bewusste Planung und Steuerung. System 2 erfordert deshalb wesentlich mehr geistige Anstrengung und Zeit. Beide Systeme sind gleichzeitig aktiv und arbeiten in der Regel reibungslos zusammen (Kahneman 2013).

2.4.2 Privatsphäre Paradox: Präferenzen und Privatheit

Westin (1967) definiert Privatheit (Privacy) „as the claim of an individual to determine what information about himself or herself should be known to others“. Oftmals treffen Individuen Entscheidungen in der digitalen Umgebung in automatisierter und gestresster Atmosphäre. Dies kann dazu führen, dass sie es verpassen, alle relevanten Informationen gleichzeitig aufzunehmen (Mirsch et al. 2018) und deshalb private Daten preisgeben, die sie unter anderen Umständen nicht zwangsläufig weitergegeben hätten. Diesbezüglich können digitale Nudges einerseits Modifizierungen hinsichtlich des präsentierten Inhalts vornehmen. Andererseits können sie die Art und Weise der Visualisierung modifizieren beispielsweise das Ändern des Designs einer Benutzeroberfläche (Schneider et al. 2018).

Insbesondere im Zusammenhang mit Entscheidungen, die die Privatsphäre betreffen, ist die menschliche Entscheidungsfindung oft unvollkommen und es werden Entscheidungen getroffen, die oft nicht den gewünschten Zielen entsprechen. Studien haben gezeigt, dass insbesondere Nutzende digitaler Systeme aufgrund kognitiver, emotionaler und sozialer Faktoren irrational handeln (Acquisti et al. 2017; Thaler and Sunstein 2009). Zum Beispiel werden personenbezogene Daten oft leichtfertig weitergegeben, weil das Risiko einer unerwünschten Überwachung geistig weniger präsent ist (Verfügbarkeitsheuristik). Diese falschen Schlussfolgerungen bedeuten nicht, dass das Verhalten der Nutzenden unberechenbar und irrational ist. Vielmehr handelt es sich um eine systematische und damit vorhersehbare Abweichung von rationalem Verhalten.

Die Forschung zum digitalen Verhalten definiert das Phänomen des Privatsphäre Paradox, d. h. die Diskrepanz zwischen der Einstellung und dem tatsächlichen Verhalten der Nutzenden in Bezug auf ihre Privatsphäre (Barth and Jong 2017). Dieses Paradoxon zeigt, dass Einzelpersonen über den Schutz ihrer Privatsphäre zwar besorgt sind. Allerdings reagieren sie nicht immer entsprechend, zum Beispiel indem sie persönliche Informationen preisgeben. Hier kommt der digitale Datenschutz ins Spiel. Privacy Nudges können beide zuvor vorgestellte Denksysteme beeinflussen, indem sie Heuristiken ausnutzen oder ihnen entgegenwirken, um Nutzende zu ihrer informationellen Selbstbestimmung zu führen (Weinmann et al. 2016). Eine Erklärung kann das Kalkül der Privatsphäre (Privacy Calculus) darstellen. Dieses Kalkül basiert auf der Tatsache, dass Individuen versuchen, den Nutzen gegen die Kosten abzuwägen. Je nachdem, ob Individuen einer Situation höhere Vorteile oder Kosten zuschreiben, entscheiden sie sich für oder gegen ein bestimmtes Verhalten. Nach dem Datenschutzparadoxon haben Individuen also mehr Nutzen als Kosten aus der Offenlegung ihrer persönlichen Informationen (Smith et al. 2011).

2.5 Digitale Arbeitssysteme

Unternehmen nutzen immer mehr Formen digitaler Arbeitssysteme, wie Slack, MS Teams oder unternehmensinterne Intranets, die den sozialen Netzwerken ähneln. Einzelpersonen nutzen diese Tools, um miteinander zu interagieren, zu arbeiten oder zu kommunizieren. Damit verbunden sind einerseits Chancen für Arbeitnehmende und Arbeitgebende, zum Beispiel durch flexiblere Arbeitsmodelle, wie Home-Office oder Crowdsourcing. Andererseits ermöglichen es diese Systeme, Informationen über Arbeitsaktivitäten sowie persönliche sensible Daten von Einzelpersonen elektronisch zu erfassen. Persönliche Nutzerinformationen werden zum Beispiel beim Anlegen eines Benutzerprofils oder beim Hochladen von persönlichen Dokumenten generiert. Hierbei besteht die Gefahr, dass die Mitarbeitenden transparent werden und somit anfällig für unerwünschte Überwachung oder Diskriminierung.

In digitalen Umgebungen neigen Einzelpersonen also dazu, unverhältnismäßig mehr Informationen preiszugeben. Die erhöhte Bereitschaft zur Selbstoffenbarung wird unter anderem auf die Tatsache zurückgeführt, dass Personen dort ein stärkeres Gefühl der Anonymität haben, soziale Anhaltspunkte im Vergleich zu Face-to-Face-Situationen schwächer sind und die Kommunikationssituation als kontrollierbar wahrgenommen wird. Daher werden digitale Arbeitsumgebungen erforderlich, die die Nutzenden bei der datenschutzfreundlichen Entscheidungsfindung unterstützen.

2.6 Datenschutz

Datenschutz ist ein nicht immer einheitlich verstandener Begriff, unter welchem sich eine Vielzahl von Schutzgütern finden lassen. Unter anderem das Recht auf informationelle Selbstbestimmung, das Recht auf Privatsphäre, Verfügungsrechte an Daten oder das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Lewinski 2020; Veil 2018). Ursprünglich wurde unter dem Begriff noch wörtlich der „Schutz von Daten“ ganz allgemein verstanden. Heute wird der Begriff des Datenschutzes jedoch als der Schutz von Persönlichkeitsrechten angesehen (Schmidt 2019b). Demnach sind nicht die Daten an sich, sondern die Grundrechte und Grundfreiheiten der natürlichen Personen hinter den Daten geschützt. Art. 8 Abs. 1 der GRC hält fest, dass jede Person das Recht auf „Schutz der sie betreffenden personenbezogenen Daten hat“. Der Schutz von Personen und nicht Daten an sich wird auch in Art. 1 Abs. 1 DSGVO deutlich. Dieser hält fest, dass die DSGVO Vorschriften zum „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ enthält (laut Schmidt (2019a) ähnlich einer Legaldefinition für Datenschutz).

Die Entwicklung des Datenschutzes nahm mit dem weltweit ersten Datenschutzgesetz, dem Hessischen Datenschutzgesetz aus dem Jahr 1970 (GVBl. II 300-10, S. 625), welches jedoch zunächst nur für öffentliche Stellen in Hessen galt, an Fahrt auf. Es handelt sich also um ein junges Rechtsgebiet (Martini and Kühling 2016). Ein weiterer Meilenstein und prägend für unser heutiges Verständnis von Datenschutz war sodann das Volkszählungsurteil vom 15. September 1983 (BVerfGE 65, 1). Mit diesem Urteil wurde das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde etabliert. Das Grundrecht gewährleistet die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ (BVerfGE 65, 1 (43)). Aufgrund der fortschreitenden Digitalisierung und Globalisierung folgten ab 1995, bedingt durch das Bedürfnis nach

mehr Einheitlichkeit und Erleichterung des innereuropäischen Datenverkehrs, auch europäische Regelungen beginnend mit der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Richtlinie 95/46/EG) bis hin zur heutigen DSGVO (Verordnung (EU) 2016/679).

3 Privacy Nudging im digitalen Kontext*

3.1 Charakterisierung von Privacy Nudges

Eine vielversprechende Methode zur Stärkung der datenschutzfreundlichen Entscheidungen ist digitales Privacy Nudging. Basierend auf den in Kapitel 2 vorgestellten theoretischen Hintergründen zu digitalem Nudging und der Entscheidungsfindung werden folgend **sieben Privacy Nudges** vorgestellt. Privacy Nudges sind eine Unterkategorie der digitalen Nudges. Privacy Nudging beschreibt eine gezielte Einflussnahme auf den Entscheidungsprozess, um Menschen zu „besseren“ Entscheidungen bezüglich ihrer Privatsphäre zu bewegen und gleichzeitig ihre informationelle Selbstbestimmung zu berücksichtigen (Acquisti et al. 2017).

Das Designelement des **Default Privacy Nudges** beschreibt die Vorauswahl von Alternativen. Da die Nutzenden die digitalen Datenschutzeinstellungen häufig nicht an ihre Bedürfnisse anpassen, wird die Standardoption (Status-quo) übermäßig bevorzugt und bleibt meist unverändert (Status-quo-Bias) (Acquisti et al. 2017; Thaler and Sunstein 2009). Darüber hinaus wird die Standardoption als Referenzpunkt für die Abwägung von Entscheidungsoptionen verwendet. Dieser „Anker“ wird von den Nutzenden unbewusst wahrgenommen. Jede Entscheidungsoption wird nun gegen diese Alternative abgewogen und das Entscheidungsverhalten in diese Richtung beeinflusst (Tversky and Kahneman 1974).

Präsentations- und Framing-Nudges beeinflussen das Entscheidungsverhalten der Nutzenden, indem zwei identische Alternativen aufgrund ihrer unterschiedlichen Präsentation wahrgenommen werden (Turland et al. 2015). Beispielsweise lenken farbige Schriftarten die Aufmerksamkeit auf ausgewählte Elemente, um bestimmte Entscheidungsalternativen hervorzuheben. Durch die Präsentation von Nudges in Kombination mit verschiedenen Farben wie roten oder grünen Elementen können diese auf unterschiedliche Weise umrahmt werden, um die Aufmerksamkeit der Nutzenden zu erregen.

Die Wahrscheinlichkeit von Verletzungen der Privatsphäre ist für die Nutzenden oft unverständlich und wird unterschätzt (Acquisti et al. 2017; Tversky and Kahneman 1974). Um diesen negativen Effekten entgegenzuwirken, wird vorgeschlagen, dass Nudges die Nutzenden von Informationssystemen über die Risiken und Konsequenzen ihrer Handlungen informieren. Auf der Grundlage dieser **Informationen** können Personen eine fundierte Entscheidung über die eigene Privatsphäre treffen (Acquisti et al. 2017).

Ein weiteres Designelement des Privacy Nudges ist die Bereitstellung von **Feedback**, welches das bisherige Nutzungsverhalten einer Person aufzeigt. Dieser Nudge-Mechanismus schafft ein Bewusstsein für die früheren und aktuellen Entscheidungen einer Person und deren Konsequenzen (Acquisti et al. 2017). Feedback-Privacy Nudges adressieren hauptsächlich Framing-Effekte, hyperbolische Diskontierung (Überschätzung des kurzfristigen Nutzens) und in weiten Teilen den Zustand unvollständiger Informationen.

Fehlerresistente Privacy Nudges können den Nutzenden helfen, da Entscheidungen zur Privatsphäre oft riskante und schlecht durchdachte Entscheidungen begünstigen, ohne mögliche langfristige Folgen zu berücksichtigen. Um dem entgegenzuwirken, kann eine **Zeitverzögerung** als Privacy Nudge eingesetzt werden (Wang et al. 2014). Auf diese Weise soll das Individuum dazu gebracht werden,

* Wesentliche Teile dieses Kapitels sind folgenden im Projekt entstandenen, gemeinsamen Publikationen entnommen: Schomberg et al. (2019); Schomberg et al. (2021); Schöbel et al. (2022).

weniger impulsiv zu handeln und die Nachricht und mögliche negative Konsequenzen zu überdenken (Acquisti et al. 2017). Um diese Eigenschaft des Privacy Nudges besser zu verstehen, widmen sich aktuelle Forschungen der Analyse der hyperbolischen Diskontierung, der Effekte der Verlustaversion und des Zustands unvollständiger Informationen (Acquisti 2009; Thaler and Sunstein 2008a; Thaler and Sunstein 2008b).

Die Wirkung des sozialen Einflusses von Privacy Nudges beruht auf dem Prinzip der **sozialen Normen**. Das Individuum leitet aus dem Verhalten seiner Mitnutzenden ab, inwieweit es angemessen ist, persönliche Informationen zu teilen (Chang et al.; Coventry et al. 2016). Die Entscheidung der Mehrheit beeinflusst die Wahrnehmung und das Verhalten der Nutzenden in einer Weise (Liu et al. 2005), dass andere das Gefühl bekommen, das Verhalten der Mehrheit nachahmen zu wollen (Coventry et al. 2016). Je mehr Menschen die gleiche Meinung zu einem bestimmten Thema haben, desto wahrscheinlicher ist es, dass sie bei anderen die gleiche Meinung hervorrufen (Wang et al. 2014), denn das Verhalten von Gleichgesinnten führt zu individuellem Verhalten (Bakshy, E., D. Eckles, R. Yan, and I. Rosenn 2012). Neben den kognitiven Effekten wird in der Forschung auch der Einfluss von Persönlichkeitsmerkmalen untersucht, die die Wirksamkeit dieses Anstoßes bestimmen, und es wird vermutet, dass Unterschiede in Persönlichkeitsmerkmalen wie Impulsivität, Kontaktfreudigkeit und Risikobereitschaft die Wirksamkeit sozialer Einflüsse beeinflussen.

Normalerweise wird ein **Fortschrittsbalken (Progress Bar)** verwendet, um den Fortschritt des Nutzenden bei der Vervollständigung eines digitalen Profils zu dokumentieren (Kroll and Stieglitz 2021). In Bezug auf den Schutz der Privatsphäre werden Fortschrittsbalken beispielsweise verwendet, um den Grad der Weitergabe von datenschutzrelevanten Informationen zu verdeutlichen oder um die Stärke von Passwörtern zu visualisieren (Khern-am-nuai et al. 2016).

3.2 Prinzipien des Privacy Nudgings

3.2.1 Rechtliche Rahmenbedingungen (DSGVO)

Nudging ist in seinem Ursprung ein „ökonomisch begreifbares Konzept zur Steuerung des menschlichen Verhaltens“ (Gerg 2019). Um die sich daraus ergebenden Rechtsfragen zu klären, schlägt der Autor eine zusätzliche rechtliche Definition des Begriffs Nudging vor. Er kommt zu dem Schluss, dass Nudging ohne wirtschaftliche Begriffe als gezielte, möglicherweise sogar unbewusste Willensmanipulation beschrieben werden kann. Das Gesetz verknüpft in der Regel positive oder negative rechtliche Konsequenzen mit einem bestimmten Verhalten. Die Personen können dann entscheiden, ob sie sich daranhalten oder nicht. Nudging beginnt jedoch früher und beeinflusst bereits den Willen eines Nutzenden selbst. Die Entscheidungen, die Nutzende treffen, werden daher in einer Weise beeinflusst, die dem Gesetz nicht bekannt ist (Gerg 2019). Diese Definition verkennt jedoch, dass Verbote und Gebote im Recht durchaus selbst Instrumente zur Verhaltenssteuerung sind (Krimphove 2017). Außerdem gibt es gesetzliche Normen, welche Nudging durch Private anordnen (beispielsweise Art. 25 Abs. 2 DSGVO). Daher ist weniger eine juristische Definition, sondern eher eine juristische Betrachtung der Sachverhalte notwendig, die nach der verhaltensökonomischen Definition als Nudging eingeordnet werden.

Der datenschutzrechtliche Rechtsrahmen für Nudging besteht im Wesentlichen aus den in Art. 5 DSGVO kodifizierten Datenschutzgrundsätzen, insbesondere dem Grundsatz der Transparenz in Art. 5 Abs. 1 lit. a DSGVO, welcher in den Normen zu den Rechten der betroffenen Personen in Art. 12 ff.

DSGVO weiter konkretisiert wird, und den Anforderungen an den Datenschutz durch Technikgestaltung und Voreinstellungen gemäß Art. 25 DSGVO. Die Datenschutzgrundsätze enthalten jedoch eine Reihe undefinierter Rechtsbegriffe und legen daher nur allgemeine Leitlinien fest, die dann in den weiteren Vorschriften der DSGVO konkretisiert werden (Laue 2019). Sobald von maßgeschneiderten Nudges die Rede ist, müssen auch die Beschränkungen für die automatisierte individuelle Entscheidungsfindung (Art. 22 DSGVO i.V.m. der rechtlichen Definition in Art. 4 Nr. 4 DSGVO) berücksichtigt werden.

Art. 25 Abs. 2 S. 1 DSGVO besagt, dass die verantwortliche Person geeignete technische und organisatorische Maßnahmen treffen muss, um sicherzustellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Daher können Nudges in Form von Voreinstellungen, die den Datenschutz fördern sollen, als Maßnahmen gemäß Art. 25 Abs. 2 DSGVO verstanden werden (Krönke 2016). Art. 25 Abs. 2 DSGVO gibt die klare Anweisung, Standardeinstellungen so datenschutzfreundlich wie möglich zu gestalten. Daher verpflichtet der europäische Gesetzgeber den Verantwortlichen, Privacy Nudges in Form von Voreinstellungen zu verwenden. Verstöße können mit hohen Geldstrafen nach Art. 83 Abs. 4 DSGVO geahndet werden. Es kann geschlussfolgert werden, der europäische Gesetzgeber schützt das Recht jeder Person auf den Schutz der sie betreffenden personenbezogenen Daten gemäß Art. 8 GRC, indem er eine Form der Privacy Nudges verpflichtend und flächendeckend vorschreibt.

Andere Ausgestaltungsarten von Nudges (zum Beispiel Framing, soziale Normen, Zeitverzögerung oder Feedback), die den Datenschutz oder die Privatsphäre fördern, können als Maßnahmen gemäß Art. 25 Abs. 1 DSGVO angesehen werden. Dieser verpflichtet den Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu ergreifen, die auf die wirksame Umsetzung der Datenschutzgrundsätze ausgelegt sind. Privacy Nudges können einen wichtigen Beitrag zur Festlegung und Umsetzung der abstrakten Anforderungen des Art. 25 DSGVO leisten, aber um einen umfassenden Datenschutz zu gewährleisten, müssen weitere technische und organisatorische Maßnahmen getroffen werden (Schomberg et al. 2019).

3.2.2 Besonderheiten digitaler Privacy Nudges

Studien haben gezeigt, dass vor allem Nutzende digitaler Systeme aufgrund kognitiver, emotionaler und sozialer Faktoren oft irrational handeln (Acquisti et al. 2017; Thaler and Sunstein 2008b). Im Alltag haben diese selten genug Zeit und Informationen, um alle Alternativen vollständig auszuwerten. Durch die Hervorhebung „populärer“ Entscheidungen wird sozialer Druck auf den die Person ausgeübt, was zu Entscheidungen führt, die manchmal nicht wirklich widerspiegeln, was Nutzende auf digitalen Plattformen wirklich wollen (Ho and Lim 2018).

Um sich besser bei der Entwicklung digitaler Nudge Konzepte zurechtzufinden, sollten Forschende mit Prozessmodellen arbeiten, die legitime Designs gewährleisten (Indulska et al. 2009). Hierbei ist jedoch anzumerken, dass die derzeitigen digitalen Nudge-Prozesse ethischen und rechtlichen Standards nicht ausreichend Rechnung tragen (Meske and Potthoff 2017; Mirsch et al. 2018), die für die Gestaltung legitimer digitaler Nudges unerlässlich sind (Spiekermann 2016). Diese beiden Aspekte sind von großer Bedeutung, da Nudging das Verhalten eines Individuums verändern und gleichzeitig das Wohlbefinden des Einzelnen erhöhen oder verringern kann.

Die Beeinflussung des Willens durch das Konzept des Nudgings ist offline wie online gleich. Die zusätzliche Gefahr in der digitalen Welt besteht jedoch in der Vernetzung verschiedenster

Datenquellen (Lobo 2017). Dies kann einerseits hilfreich sein, um Nudges exakt auf die Bedürfnisse der Nutzenden zuzuschneiden, andererseits ist es paradox, wenn zum Schutz personenbezogener Daten mehr personenbezogene Daten benötigt werden (Sandfuchs und Kapsner 2018). Durch die Vernetzung verschiedenster Quellen werden immer mehr Details über die Nutzenden gesammelt, welche eine umso präzisere Personalisierung ermöglichen. Hinzukommt, dass sich Benutzeroberflächen in der digitalen Welt gezielt und einfach testen und somit noch weiter personalisieren lassen (Weinzierl 2020).

Gemäß Art. 22 Abs. 1 DSGVO hat die betroffene Person „das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtlicher Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“. Profiling ist dabei eine automatisierte Verarbeitung der erhobenen Daten mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (siehe Art. 4 Nr. 4 DSGVO). Dies würde bei personalisiertem Nudging zutreffen, da dieses ein Profil erfordert, um Annahmen darüber zu treffen, was die Nutzenden am besten nudgen würde. Hingegen ist zweifelhaft, ob es bei libertären Nudges überhaupt zu einer Entscheidung der verantwortlichen Person kommt, da der genudgte Person immer die Möglichkeit offenbleibt, sich gegen die beabsichtigte Verhaltensweise zu entscheiden. Demzufolge ist Art. 22 DSGVO auch auf benutzerdefinierte Nudges nicht anwendbar, da die Nutzenden weiterhin selbst entscheiden (siehe für das parallele Beispiel der personalisierten Werbung Art. 22 DSGVO in Paal und Pauly 2018). Denkbar erscheint zwar, dass es durch eine sehr genaue Personalisierung für die Nutzenden schwer werden könnte, Nudges zu widerstehen. In diesem Fall ließe sich vertreten, dass die Entscheidung doch auf die Person, die den Nudge einsetzt, verlagert wird und ihr zumindest eine Beeinträchtigung innewohnt, die einer rechtlichen Wirkung gleichkommt, weil die genudgte Person nach persönlicher Empfindung keine Wahlmöglichkeit mehr hat. Gerade im Bereich der Privacy Nudges wird dies jedoch regelmäßig nicht der Fall sein. Werden die Nutzenden beispielsweise durch einen guten Privacy Nudge dazu bewogen, ein Bild nicht frei im Internet zu teilen, sondern den Empfängerkreis auf enge Freunde zu beschränken, so kommt es zu keiner erheblichen Beeinträchtigung für die Nutzenden. Dies gilt zumindest dann, wenn der Nudge die weiteren Anforderungen des Datenschutzrechts (vor allem hinsichtlich der Transparenz) einhält. Mögliche Konflikte mit dem Prinzip der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO müssten für jedes Szenario einzeln diskutiert werden.

3.2.3 Privacy Nudges im digitalen Arbeitskontext

In der ethischen Debatte werden Nudges als Mittel zur Verbesserung der öffentlichen Ordnung und damit als staatliches Instrument angesehen. Dies führt zu der Frage, ob sich die Bewertung ändert, wenn stattdessen ein Unternehmen seine Kundinnen und Kunden oder Mitarbeitenden nudged (wobei Nudging in einem paternalistischen Sinne verstanden wird). Wenn überhaupt, haben Regierungen oder staatliche Institutionen das Recht sich in das Leben der Bürgerinnen und Bürgern einzumischen und zu nudgen, da diese besondere rechtliche und ethische Verpflichtungen gegenüber ihren Bürgerinnen und Bürgern haben. Unternehmen haben zwar Verpflichtungen gegenüber Kundinnen und Kunden (zum Beispiel im Bereich der Produktsicherheit oder des Verbraucherschutzes) und ihren Mitarbeitenden (zum Beispiel Arbeitssicherheit). Dennoch sind sie vor allem daran interessiert, Profit zu machen. Auch wenn ein Nudge mit den besten Absichten entworfen wird, sind die Beweggründe dahinter gemischt – der Nudge ist womöglich Teil des Geschäftsmodells. Angesichts des jüngsten Aufschwungs von Unternehmen, die einen nachhaltigeren Lebensstil bei ihren Kundinnen

und Kunden fördern wollen, dürfte die Ethik in Zukunft zunehmend im Rahmen von Nudging oder Unternehmenspaternalismus Beachtung finden (Schöbel et al. 2020).

Nicht nur aus ethischer, sondern auch aus rechtlicher Sicht besteht eines der größten Probleme von Nudges darin, dass sie (libertär) paternalistisch sind. Staatliche Bevormundung ist in der Regel unzulässig, weil sie gegen den aus dem Rechtsstaatsprinzip abgeleiteten Grundsatz der Verhältnismäßigkeit verstößt (Gerg 2019). Auch aus rechtlicher Sicht kann Nudging durch Private (zum Beispiel Arbeitgebende oder Dienstleistende) besondere Fragen aufwerfen. Zwar ist nur der Staat unmittelbar an Grundrechte gebunden (Kirchhof 2015), diese wirken sich aber auf das Verhältnis zwischen Privatpersonen aus, da alle Gesetze verfassungsrechtlichen Vorgaben entsprechen müssen und insbesondere Generalklauseln Einbruchstellen für den Rechtsgehalt der Grundrechte sind (mittelbare Drittwirkung; grundlegend BVerfGE 7,198 – Lüth).

Sofern Private in digitalen Umgebungen nudgen, müssen sie einerseits datenschutzrechtliche Vorgaben eingehalten, andererseits könnten durch Nudges jedoch auch datenschutzrechtliche Vorgaben umgesetzt werden (Sandfuchs and Kapsner 2018). Der Rechtsrahmen für digitales Nudging (siehe 2.2.1) besteht auch in digitalen Arbeitsumgebungen im Wesentlichen aus den in Art. 5 DSGVO kodifizierten Grundsätzen für die Verarbeitung (insbesondere Grundsatz der Transparenz in Art. 5 Abs. 1 lit. a DSGVO, welcher in den Normen zu den Rechten der betroffenen Personen in Art. 12 ff. DSGVO weiter konkretisiert wird) und den Anforderungen an den Datenschutz durch Technikgestaltung und Voreinstellungen gemäß Art. 25 DSGVO. Sobald es um maßgeschneiderte Nudges geht, müssen auch die Beschränkungen für die automatisierte Entscheidung im Einzelfall (Art. 22 DSGVO i.V.m. der Legaldefinition in Art.4 Nr. 4 DSGVO) berücksichtigt werden.

Seit dem 25.05.2018 gilt die DSGVO als Verordnung unmittelbar und muss, im Gegensatz zu einer Richtlinie, nicht durch den nationalen Gesetzgeber umgesetzt werden. Sie genießt einen Anwendungsvorrang gegenüber nationalen Regelungen. Es gibt jedoch in der DSGVO eine Vielzahl von Öffnungsklauseln, welche den Mitgliedstaaten wiederum Raum für nationale Regelungen gewähren (Martini and Kühling 2016). Eine dieser Öffnungsklauseln ist Art. 88 DSGVO, welcher es den Mitgliedstaaten erlaubt, „spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von personenbezogenen Beschäftigtendaten im Beschäftigungskontext“ zu erlassen. Durch diesen Wortlaut wird indiziert, dass keine wesentlichen inhaltlichen Abweichungen von den allgemeinen Vorgaben der DSGVO erlaubt sind (Kort 2017; Wybitul 2017). Art. 88 Abs. 2 DSGVO schreibt vor, dass die nationalen Vorschriften „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen“ umfassen.

Der deutsche Gesetzgeber hat davon in § 26 BDSG Gebrauch gemacht und orientierte sich dabei erkennbar an § 32 BDSG a.F., welcher zuvor den Beschäftigtendatenschutz regelte (Wybitul 2017). So wurde der Kern der alten Regelung übernommen und es werden nach wie vor alle drei Phasen des Beschäftigungsverhältnisses, nämlich die Begründung, dessen Durchführung und dessen Beendigung, erfasst. Diese strukturelle Ähnlichkeit soll für eine gewisse Kontinuität im deutschen Beschäftigtendatenschutz sorgen (Kort 2018). Inhaltlich geht die neue deutsche Regelung des Beschäftigtendatenschutzes jedoch deutlich über die bisherige hinaus (Kort 2017).

§ 26 Abs. 2 BDSG stellt klar, dass Beschäftigte auch weiterhin im Rahmen des Beschäftigungsverhältnisses in die Verarbeitung ihrer personenbezogenen Daten einwilligen können. Dies ergibt sich zudem schon aus Erwägungsgrund 155 der DSGVO und entspricht auch der bisherigen Rechtsprechung des Bundesarbeitsgerichts. Um dem Über-/Unterordnungsverhältnis von

Arbeitgebenden und Arbeitnehmenden Rechnung zu tragen, werden mit Art. 26 Abs. 2 BDSG jedoch erhöhte Anforderungen an die Freiwilligkeit der Einwilligung gestellt. Arbeitgebende müssen bei der Beurteilung der Freiwilligkeit immer die im Beschäftigungsverhältnis bestehende Abhängigkeit der Beschäftigten berücksichtigen. Von der Freiwilligkeit der Einwilligung ist jedoch auszugehen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder sofern Arbeitgebende und Beschäftigte gleichgelagerte Interessen verfolgen (Wybitul 2017). Eine Einwilligung der Arbeitnehmenden in die Verarbeitung ihrer personenbezogenen Daten mit inkludierten Privacy Nudges dürfte daher unproblematisch möglich sein, da in der Regel sowohl Arbeitgebende als auch Arbeitnehmende ein Interesse an datenschutzfreundlicher Ausgestaltung der Datenverarbeitung haben. Beschäftigte müssen jedoch über ihr Widerrufsrecht gemäß Art. 7 Abs. 3 DSGVO aufgeklärt werden.

Die Rolle des Betriebsrats war lange unklar. Weder die DSGVO noch § 26 BDSG befassen sich mit der Frage, ob der Betriebsrat eigenständiger Datenverarbeiter oder Teil des Arbeitgebenden als der für die Datenverarbeitung Verantwortliche ist (Kort 2017; Kort 2018). Seit 2021 ist nunmehr geregelt, dass der Arbeitgeber Verantwortlicher im Sinne der DSGVO bleibt, wenn der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben Daten verarbeitet (§ 79a S. 2 BetrVG, vgl. auch § 69 S. 2 BPersVG für Personalrat und Dienststelle). Der Betriebsrat hat jedoch die Vorschriften über den Datenschutz einzuhalten (§ 79a S. 1 BetrVG) und Arbeitgebende und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften (§ 79a S. 3 BetrVG). Der Betriebsrat könnte gemäß § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht bei der Ausgestaltung von digitalen Nudges haben. Privacy Nudges dürften für den Betriebsrat jedoch durchaus zustimmungsfähig sein. Bei Beachtung der überschaubaren Besonderheiten des Beschäftigungsdatenschutzes mit Relevanz für Nudging stehen auch Art. 88 DSGVO und § 26 BDSG der Umsetzung der Vorgaben der DSGVO durch Privacy Nudges nicht entgegen.

4 Systematisches Design von digitalen Privacy Nudges

4.1 Anforderungen an das Design und die Implementierung

Die Interviewergebnisse wurden mit den Ergebnissen der systematischen Literaturrecherche konsolidiert, um die Anforderungen für das Modell abzuleiten. Mehr als 26 Designanforderungen (DA) wurden gesammelt, auf Redundanz geprüft und zu 15 vorläufigen Modellanforderungen zusammengefasst. Sie wurden zur besseren Verständlichkeit komprimiert und vereinfacht, um ihren Nutzen für Architekten zu gewährleisten (siehe Tabelle 1). Diese bilden zudem die Grundlage für die Inhalte in Kapitel 5.

Tabelle 1: Design Anforderungen

Problemkategorie	Designanforderung (DA)	Quelle
Kontext der Entscheidung	DA1: Der Erstellungsprozess sollte den Kontext des digitalen Nudges berücksichtigen.	Experteninterviews and Literatur
Ausrichtung des Nudges auf angrenzende Bereiche	DA2: Digitale Nudges sollten mit unterstützenden Aktivitäten, Geschäftsprozessen und der Gesamtstrategie abgestimmt werden. DA3: Die Verbesserung des Nudges sollte z.B. durch künstliche Intelligenz in Betracht gezogen werden. DA4: Nudge-Designerinnen und -Designer müssen die Ziele, Werte und Präferenzen der Nutzenden verstehen. Nudges sollten dementsprechend ausgerichtet sein.	Experteninterviews and Literatur
Anpassungsfähigkeit des Nudges	DA5: Unterschiedliche Merkmale der Nutzenden sollten berücksichtigt werden. DA6: Es sollten verschiedene technologische Merkmale berücksichtigt werden.	Experteninterviews and Literatur
Legitimität des Nudges	DA7: Digital Nudges sollten hohen ethischen Standards entsprechen. DA8: Digital Nudges sollten hohen rechtlichen Standards entsprechen. DA9: Digitale Nudges sollten hohen psychologischen Standards entsprechen. DA10: Digitale Nudges sollten sich an hohen gesellschaftlichen Standards orientieren.	Experteninterviews and Literatur
Effektivität des Nudges	DA11: Der Prozess sollte die Gestaltung und Umsetzung digitaler Nudges verbinden. DA12: Nudge-Designerinnen und -Designer sollten den Zeitplan berücksichtigen, da der Erfolg einiger digitaler Nudges von ihrer rechtzeitigen Umsetzung abhängt.	Experteninterviews and Literatur
Benutzerfreundlichkeit des Nudges im System	DA13: Die Erstellungsprozesse sollten einfach zu verstehen und in der Praxis nachvollziehbar sein. DA14: Eine Kosten-Nutzen-Analyse sollte berücksichtigt werden.	Experteninterviews and Literatur
Evaluierung des Nudges	DA15: (Nutzenden-)Feedback und neue Erkenntnisse sollten kontinuierlich in den Prozess integriert werden.	Experteninterviews and Literatur

Je nach Einsatzszenario ergibt sich eine andere Gestaltungsgrundlage für die Auswahl von digitalen Nudges. Nudges können sowohl online als auch offline genutzt werden. Die soziotechnische Perspektive fokussiert sich primär auf den digitalen Kontext und digitale Umgebungen. Hingegen gelten die ethische und rechtliche Sichtweise zumindest hinsichtlich der grundsätzlichen Probleme des Paternalismus sowohl für Nudges im digitalen als auch im realen Bereich. Bevor ein Nudging Konzept entwickelt wird, ist es wichtig, sich das Ziel des Nudgings und den Kontext des Einsatzes vor Augen zu führen. Dies ist von Bedeutung, um rechtliche und ethische Grauzonen auszuschließen und von Beginn

der Entwicklung eines Nudging Konzeptes entsprechende Maßnahmen in Bezug auf die Gestaltung treffen zu können. Außerdem ist die Entwicklung eines digitalen Nudging-Konzepts komplex, da viele verschiedene Aspekte berücksichtigt werden müssen. Zum Beispiel sollte der Nudge transparent und für die Nutzenden sichtbar sein, da Kritikerinnen und Kritiker andernfalls zu dem Schluss kommen könnten, dass Nudges einen manipulativen Charakter haben und die Autonomie des Einzelnen untergraben.

Folglich bedeutet dies:

- Vor der Entwicklung eines Nudging Konzeptes sollten das Einsatzszenario und das Ziel des Konzeptes erörtert werden, um Gestaltungsansätze auszuschließen, die rechtlich und ethisch nicht konform sind und solche Ansätze zu wählen, die die gewünschten Nutzungseffekte erzielen, also zum Datenschutz beitragen (Schöbel et al. 2020).
- Digitale Nudges erfordern es, ethische, rechtliche und soziotechnische Aspekte für die Gestaltung zu berücksichtigen, um Nutzende bei Entscheidungen, die sie in digitalen Umgebungen treffen müssen, zu unterstützen (Schöbel et al. 2020).
- Digitale Nudges sollten unter Berücksichtigung von ethischen und rechtlichen Fragestellungen auf die Interessen und Bedürfnisse der Nutzenden abgestimmt werden, um Nutzende bei ihren Handlungen zum Schutz ihrer Daten zu unterstützen (Schöbel et al. 2020).
- Nudge Elemente sollten so ausgewählt und kombiniert werden, dass diese rechtliche, ethische und soziotechnische Kriterien bei der Gestaltung berücksichtigen, um ihre Effektivität im Sinne des Schutzes von Nutzerdaten zu unterstützen (Schöbel et al. 2020).

4.2 Design Prinzipien für digitale Privacy Nudges

Auf der Grundlage der entwickelten Designanforderungen konnten Designprinzipien für die Gestaltung von Privacy Nudges entwickelt werden. Dazu wurde eine systematische Literaturrecherche nach der von Vom Brocke et al. (2009) vorgeschlagenen Methodik durchgeführt und 38 relevante Arbeiten identifiziert. Um die Ergebnisse zu erweitern und zu validieren, wurden verschiedene Expertenworkshops durchgeführt. Die vorläufigen Ergebnisse schlagen Gestaltungsanforderungen vor, die wirksame Privacy Nudges in modernen Arbeitssystemen erfüllen sollten. Ein Auszug aus den Gestaltungsprinzipien ist in Tabelle 2 aufgeführt.

Tabelle 2: Design Prinzipien

Design Anforderung	Design Prinzipien
Benutzerfreundlichkeit	DP1) Gewährleistung eines ergonomischen und leicht zugänglichen Designs DP2) Reibungslose Integration von Nudges in Arbeitsabläufe
Transparenz	DP3) Konzentration auf relevante Informationen für datenschutzfreundliche Entscheidungen DP4) Informationen darüber geben, warum und wofür der Nudge gedacht ist DP5) Abwägen von Informationen zum Schutz der Privatsphäre und wirtschaftlichen Interessen
Interaktion	DP6) Bevorzugte Verwendung von Default- und Framing-Nudges DP7) Datenschutz und Datenschutzrisiken konkretisieren und tangibel gestalten
Anpassungsfähigkeit	DP8) Personalisierung von Nudges
Wirtschaftlichkeit	DP9) Das Geschäftsmodell des Unternehmens nicht blockieren DP10) Design- und Implementierungskosten für die Machbarkeit und Implementierung von Nudges sicherstellen

5 Kodifizierung des Gestaltungswissens

Für die Gestaltung neuartiger Systeme wird die Kodifizierung von Gestaltungswissen für die Forschung und Praxis immer wichtiger (Gregor and Jones 2007). Dabei werden Regeln und Konzepte wie Designtheorien und Designprinzipien angewandt, die zur Abbildung und Unterstützung von Designprozessen genutzt werden können (Peppers et al. 2007). So akkumulieren viele Projekte Gestaltungswissen, indem sie Artefakte wie Theorien über verschiedene Projekte und Publikationen hinweg bauen, evaluieren und verbessern (Gregor and Hevner 2013). Die Sammlung und Kodifizierung von Wissen ist ein Grundstein für Theorien und erfordert verschiedene Herangehensweisen (Gregor 2006). Ein Ziel des Nudger Projektes bestand darin, das interdisziplinär entwickelte Gestaltungswissen zu sammeln und in einer nützlichen Darstellungsweise anderen zugänglich zu machen.

Bevor genauer auf die Kodifizierung des Gestaltungswissens eingegangen wird, wird zunächst erläutert, was Gestaltungswissen eigentlich ist und wie das Wissen generiert wird. Die Fähigkeit, Wissen zu schaffen und zu nutzen, ist zu einer der wichtigsten menschlichen Eigenschaften geworden (Nonaka and Toyama 2003). Wird eine Person nach dem Grund für ihre Entscheidung gefragt, so sagt sie oft, dass die Entscheidung aufgrund eines Gefühls getroffen wurde. Bauchgefühle entstehen in der Regel durch Erfahrung und lassen sich nur schwer weitergeben, da der Besitzer Schwierigkeiten hat, sie auszudrücken. In der Literatur wird der Begriff „implizites Wissen“ verwendet. Das implizite Wissen ist schwer zu formulieren und zu kodifizieren, während das explizite Wissen zugänglich und daher leicht zu kodifizieren ist. Forschende neigen dazu, implizites Wissen über explizites Wissen zu stellen und sich auf ersteres zu konzentrieren (Alavi and Leidner 2001). Wissen wird von einer Person geschaffen und wird wertvoll, wenn sie es mit anderen Personen teilt (Nonaka and Takeuchi 1995). Während explizites Wissen leicht übertragen werden kann, ist implizites Wissen schwer zu übertragen (Müller and Thoring 2010).

Gestaltungswissen ist eine besondere Form von Wissen, nämlich das Wissen um die Gestaltung eines Systems inklusive der Methodiken (Gregor and Hevner 2013). *Van Aken* definiert Gestaltungswissen als „[...] Wissen, das zur Erstellung von Designs verwendet werden kann. Das allgemeine Gestaltungswissen im Repertoire des Gestalters wird von ihm bzw. ihr im Laufe der Jahre aufgebaut“ (van Aken 2005).

5.1.1 Entwicklung von Nudge Entwurfsmustern

Gestaltungswissen hat bestimmte Eigenschaften, die seine Weitergabe erschweren, insbesondere wenn es nicht in kodifizierter Form vorliegt (Müller and Thoring 2010). Um Gestaltungswissen für die Zukunft wiederverwendbar zu machen, muss es zunächst externalisiert, erfasst und dann an andere Personen weitergegeben werden (Faraj and Sproull 2000). Heute gibt es eine Fülle von Möglichkeiten, Gestaltungswissen zu sammeln und zu kodifizieren, zum Beispiel Designprinzipien, Design Pattern und Designtheorien. Es sind zwei Dinge wichtig, um Gestaltungswissen nutzbar und zugänglich zu machen, damit es in neuen Anwendungskontexten gemeinsam genutzt und wiederverwendet werden kann. Erstens muss das Werkzeug, in dem das Wissen kodifiziert ist, den Nutzenden in die Lage versetzen, die erforderlichen Informationen in kürzester Zeit zu finden. Zweitens ist die Aufbereitung des Konstruktionswissens vor der Kodifizierung entscheidend. Bevor jedoch Gestaltungswissen kodifiziert werden kann, muss entschieden werden, wie wir die Informationen kommunizieren, um sie für andere anwendbar zu machen.

Sobald Wissen kodifiziert ist, wird es zu Informationen (McLure-Wasko 1999). Die Herausforderung bei der Weitergabe von Wissen besteht darin, dass die Information erst dann wieder zu Wissen wird, wenn eine andere Person in der Lage ist, die Information zu erfassen. Damit theoretisches Wissen in der Praxis einen Mehrwert hat, muss es an den jeweiligen Kontext angepasst werden. Herausforderungen ergeben sich vor allem bei der Anwendung von theoretischem Wissen (Lukyanenko and Parsons 2020).

Da Wissen oft nur vage formuliert ist, erfordert die Kodifizierung von Designwissen besondere Methoden. In der Systementwicklung sind (Entwurfs-)Muster eine Lösung für wiederkehrende Probleme und Herausforderungen (Gamma 1995). Entwurfsmuster haben ihren Ursprung in den Arbeitenden rund um *Alexander* (1977) auf dem Gebiet der Stadtarchitektur. Entwurfsmuster sind etablierte Werkzeuge, um komplexes Wissen für Systementwickler zugänglich zu machen. In der Literatur werden sie oft als „Schablonen“ von etablierten Lösungen für häufig wiederkehrende Probleme in der Systementwicklung bezeichnet. Entwurfsmuster enthalten Schablonen zur Beschreibung von Informationen in Tabellenform und stellen etablierte Instrumente dar, um komplexes Wissen für Entwicklerinnen und Entwickler zugänglich und anwendbar zu machen. Darüber hinaus dokumentieren Entwurfsmuster bekannte und bewährte Problemlösungen (Gamma 1995).

Color Framing Nudge		Nudge Mechanism	
		<input checked="" type="checkbox"/> unterstützend	<input type="checkbox"/> konfrontierend
		<input type="checkbox"/> verstärkend	<input type="checkbox"/> Angst machend
			<input type="checkbox"/> sozialer Einfluss
			<input type="checkbox"/> täuschen
Zielzustand			
Die Farbauswahl beeinflusst den Nutzenden möglichst datenschutzfreundlich zu handeln.			
Einflüsse		Konsequenzen	
Die Darstellung und die Farbwahl der Website muss berücksichtigt werden: Viele verschiedene Farben können den Nudgeeffekt beeinflussen.		Der Nudge beeinflusst die Handlung des Nutzenden. Der Nutzende kann beeinflusst werden möglichst datenschutzfreundlich zu handeln.	
Risiken, die berücksichtigt werden müssen			
Der Effekt des Nudges kann gegenteilig ausgenutzt werden. Wenn der Nutzende mit der Farbe grün etwas positives beabsichtigt, neigt er dazu den grünen Button anzuklicken – unabhängig von der Auswirkung. Achtung bei rot-grün Schwäche.			
Nudge Design			
Die Farbauswahl sollte mit der assoziierten Wirkung einhergehen, d.h. grüne Farben assoziieren eine datenschutzfreundliche Entscheidung und rot das Gegenteil. Es sollte darauf geachtet werden möglichst wenige personenbezogene Daten zu sammeln. Die Gestaltung sollte dabei so transparent wie möglich sein, sodass der Nutzende eine informierte Entscheidung treffen kann.			

Abbildung 1: Eigene Darstellung. Entwurfsmuster „Color Framing Nudge“

Entwurfsmuster wurden im Nudger Projekt eingesetzt, um das interdisziplinär erworbene Gestaltungswissen zu sammeln und weiteren Personen zugänglich zu machen. Im Folgenden wollen wir das Entwurfsmuster „Color Framing“ (siehe Abbildung 1) genauer vorstellen. Der Nudge „Color Framing“ lenkt die Aufmerksamkeit des Nutzenden durch eine clevere Farbwahl auf bestimmte Elemente und kann den Nutzenden so beispielsweise zu einer datenschutzfreundlicheren Handlung beeinflussen. Hierbei werden oftmals die Farben rot und grün verwendet, die entweder mit „Achtung“ oder „es ist alles gut“ assoziiert sind.

Für die Umsetzung des Nudges ist jedoch die Berücksichtigung der Gesamtheit der Website oder Applikation erforderlich. So hängt beispielsweise die Farbwahl von der Gesamtdarstellung der Website ab. Ist eine Website bereits sehr bunt oder die hauptsächlich verwendete Farbe ist grün, dann ist der Effekt eines grünen Buttons geringer als auf einer Website, die hauptsächlich grau verwendet.

5.1.2 Entwurfsmuster für die Gestaltung datenschutzgerechter Videokonferenzsysteme

Zuvor wurde gezeigt, wie Entwurfsmuster Gestaltungswissen für die Erstellung von Privatsphäre freundlichen Nudges kodifizieren können. Im Folgenden wollen wir nun spezifische Entwurfsmuster für die Gestaltung eines datenschutzgerechten Videokonferenzsystems erstellen. Videokonferenzsysteme sind unter anderem durch die Corona Pandemie zu einem festen Bestandteil in vielen Berufswelten geworden. Jedoch ermöglichen Videokonferenzen in privatem Umfeld auch vermehrte Einblicke in das private Leben und gewähren möglicherweise auch ungewollt die Erhebung besonders schützenswerter Daten. Um dies zu verhindern kann ein virtueller Hintergrund hilfreich sein. Die Verwendung des virtuellen Hintergrundes kann durch einen Nudge unterstützt werden.








Virtueller Hintergrund 		Einsatzzeitpunkt 	
		<input checked="" type="checkbox"/> Vor der Videokonferenz <input type="checkbox"/> Während der Videokonferenz <input type="checkbox"/> Nach der Videokonferenz	
Zielzustand 			
Als Nutzer möchte ich die Vorteile der Videokonferenzen nutzen, ohne dabei unnötige sensible Daten preiszugeben.			
Problem 			
Das Einschalten der Videokamera in Videokonferenzen fördert die digitale Zusammenarbeit, da sowohl die Mimik als auch die Gestik des Gegenübers wahrgenommen werden können. Jedoch können durch das Teilen der Umgebung private (oftmals sensible) Einblicke gegeben werden. Darunter können Fotos, andere Personen oder private Umgebungen, die Rückschlüsse schließen lassen, sein.			
Einflüsse 		Konsequenzen 	
Die automatische Erkennung der Person kann je nach Hintergrund dennoch vereinzelt Einblicke in das private Umfeld geben.		Die Auswahl des virtuellen Hintergrundes nimmt zu Beginn der Videokonferenz Zeit in Anspruch.	
Lösung 			
<ul style="list-style-type: none"> • Die Default-Einstellung schaltet sowohl die Kamera als auch den Ton aus • Bei Anschalten der Kamera wird die Nutzung eines virtuellen Hintergrundes vorgeschlagen, um keine kritischen Einblicke in die Umgebung zu gewähren • Bevor die Kamera eingeschaltet wird, wird die zu teilende Ansicht dargestellt, um im Falle einer Entscheidung gegen einen virtuellen Hintergrund Bewusstsein über die Ansicht der Kamera zu zeigen • Nudging durch die Empfehlung eines virtuellen Hintergrundes 			
Bestätigung der Umsetzung des Design Patterns		Datum	Unterschrift

Abbildung 2: Eigene Darstellung. Entwurfsmuster „Virtueller Hintergrund“

Das Entwurfsmuster „Virtueller Hintergrund“ (siehe Abbildung 2) stellt die Gestaltung möglicher Nudging Elemente zur Auswahl eines virtuellen Hintergrundes vor, um das notwendige Gestaltungswissen für die Umsetzung des Nudges zu vermitteln. Neben einem eindeutigen Namen wird im Entwurfsmuster der Einsatzzeitpunkt des Nudges während der Videokonferenz vorgestellt. Der Nudge setzt an der Interaktion an, bevor das Bild der Kamera der teilnehmenden Person für alle sichtbar ist, indem diese dazu aufgefordert wird, bei Einschalten der Kamera in der Videokonferenz einen virtuellen Hintergrund auszuwählen. Der Zielzustand demonstriert die bestmögliche Situation der Gestaltungslösung nach Umsetzung des Entwurfsmusters. So sollen die Nutzenden des

Videokonferenztools die Möglichkeit haben an der Konferenz teilzunehmen, ohne dabei unnötige Daten ihres privaten Umfelds preiszugeben.

6 Das DELEN Modell

Mit der Entwicklung des DELEN-Modells wird ein Beitrag zu Theorie und Praxis geleistet, indem ein digitales Nudging-Prozessmodell bereitgestellt wird, das eine legitime und effektive Gestaltung und die Entwicklung von digitalem Nudging fördert.

Der allgemeine Prozess der Entwicklung digitaler Nudges beginnt mit einer Phase der Problemerkennung gefolgt von der Phase der Zielsetzung. In diesen Phasen sollten Entscheidungsbeeinflussende das spezifische Verhalten, das sie ändern wollen, identifizieren und sich darauf konzentrieren. In unserem Modell konzentrieren wir uns auf die Design- und Entwicklungsprozesse und stellen diese im Detail vor, da sie der Schlüssel zur Erstellung digitaler Nudges sind. Nach jedem Prozess können die entwickelten Nudges in einer künstlichen Umgebung bewertet und überarbeitet werden. Anschließend können die entwickelten Nudges in das System implementiert und in einer realen Umgebung bewertet werden. Das vollständige Modell ist in Abbildung 3 dargestellt.

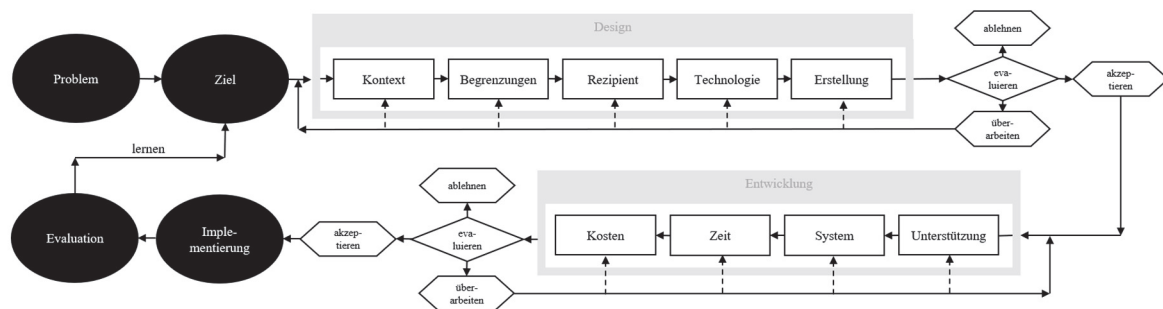


Abbildung 3: Eigene Darstellung. DELEN Prozessmodell

Der Designprozess beschreibt, wie digitale Anregungen systematisch erstellt werden können. Er umfasst fünf Schritte, die nacheinander durchgeführt werden sollten und im Folgenden erläutert werden. Das Design basiert dabei auf den in Kapitel 4 abgeleiteten DAs.

6.1 Designprozess

Bewertung des Kontextes: Zunächst sollten die Entscheidungsbeeinflussende den Weg des Nutzenden darstellen (siehe DA1, Tabelle 1). So lässt sich feststellen, zu welchem Zeitpunkt das Individuum Entscheidungen trifft und die optimalen Zeitpunkte für die Umsetzung von Maßnahmen können somit ermittelt werden. Gleichzeitig sollten die Prozesse identifiziert werden, in denen keine Intervention durchgeführt werden muss, um nicht mit anderen Prozessen zu interferieren. Dabei sollte die spezifische Entscheidungsarchitektur analysiert werden, um relevante Kontextfaktoren zu identifizieren, die die Entscheidungsfindung des Individuums bestimmen (Barev et al. 2021).

Festlegung der normativen Grenzen: Um legitime Nudge-Designs zu entwerfen, sollten Entscheidungsbeeinflussende die ethischen (siehe DA7), rechtlichen (siehe DA8), psychologischen (siehe DA9) und gesellschaftlichen Normen (siehe DA10) zusammenstellen, die den Rahmen für den digitalen Nudge bilden. Es ist wichtig zu betonen, dass diese Elemente je nach

Entscheidungsarchitektur unterschiedlich sein können und stark kontextabhängig sind. So gelten beispielsweise für Unternehmen und Regierungen unterschiedliche rechtliche Bedingungen (siehe oben). Trotzdem sollten Nudge-Designer und Designerinnen normative Grenzen für den bewerteten Kontext ermitteln und festlegen.

Zielgerichtete Ansprache der Empfänger: Viele Nudges zeigen eine geringere Wirksamkeit, da sie meistens nicht zielgruppenspezifisch designt wurden. Daher ist es wichtig, ein Verständnis für die kognitiven und affektiven Prozesse der Nutzenden zu entwickeln und welche Heuristiken zugänglich sind (siehe DA5). Sundar et al. stellen fest, dass Personen mit einem stärkeren Glauben an die interne Logik einer bestimmten Heuristik eher dazu neigen, diese Heuristik aufzurufen, wenn ihnen ein Hinweis präsentiert wird, verglichen mit Personen mit einer schwächeren Überzeugung (Sundar et al. 2020). Um also eine höhere Effektivität von Nudges zu erreichen, sollten die Nutzenden segmentiert und entsprechend angesprochen werden, da einige Personen durch digitale Nudges zielgerichteter angesprochen werden können als andere. Die Zielgruppe sollte eng gefasst sein, da ineffektive Nudges Arbeitsprozesse verlangsamen oder das Individuum negativ stimulieren können. Es ist wichtig sicherzustellen, dass das beabsichtigte Verhalten mit den Vorlieben und Werten der angestoßenen Person übereinstimmt (siehe DA4). Dies ist von entscheidender Bedeutung, da es sich hierbei um wichtige Aspekte der ethischen Rechtfertigung und Legitimität von digitalen Nudge-Designs handelt.

Anpassen an die Technologie: Entscheidungsbeeinflussende sollten sich auf die besonderen Eigenschaften der verwendeten Technologie konzentrieren und berücksichtigen, wie jedes Individuum mit ihr interagiert (siehe DA6). Nudges sollten anders gestaltet werden, wenn die Technologie visuelles, auditives oder haptisches Feedback oder haptische Rückmeldung geben kann. So kann beispielsweise ein Stoppsignal durch einen roten Knopf (visuell), einen Alarm-Ton (auditiv) oder einen Schüttelimpuls (haptisch) übermittelt werden. Außerdem kann ein Nudge auf einem festen Gerät anders aussehen als auf einem mobilen Gerät.

Erstellung des digitalen Nudges: Auf der Grundlage der vorherigen Analyse können die Entscheidungsbeeinflussende nun das geeignete Nudge-Element auswählen. Wie bereits vorgestellt, können hier beispielsweise Nudge-Elemente wie die Standardeinstellungen, die Rahmung einer Entscheidung oder die farbliche Hervorhebung der vorteilhaften Option in Betracht gezogen werden.

6.2 Implementierungsprozess

Der Entwicklungsprozess besteht aus vier Elementen und ist eine Vorstufe der Umsetzungsphase, in der die Faktoren berücksichtigt werden, die für eine wirksame Umsetzung festgelegt werden müssen. Die Entwicklung ist eng mit dem Nudge-Design verknüpft, so dass die Entscheidungsbeeinflussende diese Prozesse in Wechselbeziehung zueinander betrachten (siehe DA11).

Unterstützung: Nudges können trotz sorgfältiger Gestaltung zu unbeabsichtigten oder widersprüchlichen Verhaltensweisen führen. Zudem können Nudges andere wichtige Ziele gefährden, zum Beispiel, wenn ein Nudge, der die Umweltverschmutzung reduzieren soll, am Ende einen anderen Faktor erhöht, wie beispielsweise die Energiekosten für die am meisten benachteiligten Mitglieder der

Gesellschaft (Sunstein and Reisch 2013). Daher können von Anfang an weitere unterstützende Mechanismen implementiert werden, um schädlichen Verhaltensweisen entgegenzuwirken (siehe DA2). Personen, die ein ungewolltes Verhalten zeigen, können wieder eingefangen und umgelenkt werden. Um dies zu erreichen, kann eine Vielzahl von Mechanismen eingesetzt werden. Entscheidungsbeeinflussende können auch andere „weiche“ oder sogar „härtere“ Mechanismen wie Gesetze oder Verordnungen in Betracht ziehen. Insgesamt sollte der eingeführte Mechanismus auf die Gesamtstrategie und die bestehenden Geschäftsprozesse abgestimmt sein, um sicherzustellen, dass das Gesamtziel erreicht wird.

System: Heute gibt es eine breite Palette von Systemen, die die Wirksamkeit der Nudges beeinflussen können. Entscheidungsbeeinflussende sollten entscheiden, inwieweit beispielsweise künstliche Intelligenz oder Big Data digitale Nudges verbessern können. Zum Beispiel weisen *Ferreya et al.* darauf hin, dass künstliche Intelligenz digitale Anstöße verbessern kann, um sie dynamisch zu machen, unter anderem in Form von Hypernudges (Ferreya et al. 2020 - 2020).

Zeit: Der Erfolg einiger digitaler Nudges hängt von ihrer rechtzeitigen Umsetzung ab. Verschiedene Forschende haben nachgewiesen, wie sich die verschiedenen Timings von Nudges auf ihre Wirksamkeit auswirken (Dalecke and Karlsen 2020). Daher ist es wichtig zu berücksichtigen, wann der Nudge im System implementiert wird und wann er dem Individuum zugänglich gemacht wird (siehe DA12). Dies kann zu jeder Tageszeit sein, beispielsweise morgens, mittags, abends oder nach besonderen Ereignissen (zum Beispiel Datenschutzskandale).

Kosten: Bei der Einführung digitaler Nudges sollten die Entscheidungsbeeinflussende die Kosten und Nutzen abwägen. Es sollte entschieden werden, ob andere Alternativen ein besseres Kosten-Nutzen-Verhältnis aufweisen und welcher Mechanismus zur Verhaltensänderung verwendet werden sollte (siehe DA14).

6.3 Überarbeitungs- und Optimierungsprozesse

Nach der Design- und Entwicklungsphase folgt eine Phase der Erprobung und Bewertung. Hier sollte der Nudge getestet und bei Bedarf angepasst werden (siehe DA15). In dieser Phase sollten die Entscheidungsbeeinflussende bewerten, ob der entwickelte Nudge beispielsweise die Randbedingungen erfüllt und wie die Nutzenden damit interagieren.

Nach dem Problemidentifizierungsprozess sollten die Nudge-Designenden testen, wie der Nudge zum Beispiel in Zusammenarbeit mit unterstützenden Mechanismen oder zu verschiedenen Zeiten in dem System funktionieren. Nach der Auswertung können die Entscheidungsbeeinflussende die verschiedenen Faktoren entsprechend anpassen und spezifische Erkenntnisse für einen weiteren Design- und Entwicklungszyklus berücksichtigen, falls erforderlich. Selbst wenn die entworfenen und implementierten Nudges scheitern (angepasst oder verworfen werden), haben die Entscheidungsbeeinflussende nun eine Methode, um mögliche Fehler oder Probleme besser zu analysieren und daraus Erkenntnisse für künftige Verbesserungen zu gewinnen.

7 Anwendung

Es soll zunächst ein Szenario vorgestellt werden, für das mit dem Prozessmodell digitale Nudges entwickelt wurden. Zur besseren Demonstration der Inhalte unseres Projektes wurde im Future Work Lab des Fraunhofer IAO in Stuttgart ein technischer Demonstrator aufgestellt, welcher Privacy Nudges im Umfeld der Anwendung Lyncronize des Praxispartners smartransfer zeigen soll.

Das Szenario des technischen Demonstrators fokussiert sich auf den Bewerbungsprozess über die Plattform Lyncronize. Für eine Bewerbung werden in der Regel eine Vielzahl an Daten von der sich bewerbenden Person benötigt. Viele dieser Daten sind notwendig für ein mögliches Zustandekommen eines neuen Beschäftigungsverhältnisses. Oft werden jedoch unnötig viele Daten preisgegeben. Im Projekt wurden daher Privacy Nudges entwickelt, welche die sich bewerbenden Personen dabei unterstützen, nur tatsächlich benötigte und für den Bewerbungsprozess relevante personenbezogene Daten preiszugeben.

Die Plattform Lyncronize funktioniert so, dass die Nutzenden ein umfassendes Profil von sich selbst anlegen können. Es gibt jedoch bisher keine Hinweise zu der unterschiedlichen Wichtigkeit der Daten für den Bewerbungserfolg. Nutzende müssen sich auf ihr jeweiliges Erfahrungslevel verlassen und abwägen, was hilfreich/notwendig ist und was nicht. Um die unterschiedlichen Erfahrungslevel der Nutzenden deutlich zu machen, wurden die Personas Fred und Ingrid in die Beschreibung des Demonstrators integriert. Bei Fred handelt es sich um einen erfahrenen Nutzenden, welcher einen selbstbewussten Umgang mit digitalen Tools gewohnt ist. Die Persona Ingrid steht hingegen eher für einen unerfahrenen und unsicheren Typ Mensch im Umgang mit Technik und digitalen Tools.

Sobald die Nutzenden ihr Profil angelegt haben, können sie über die Funktion „Matching“ nach zum Profil passenden Projektvorschlägen suchen. Die Nutzenden können dabei alle gefundenen Projekte miteinander vergleichen und einzelne Projekte favorisieren. Durch Klicken auf ein Projekt werden zusätzliche Details angezeigt. Auch in diesem Stadium können die Skills noch nachjustiert werden. So lässt sich direkt erkennen, welche Veränderung der Skills eine Veränderung des Projektangebots zur Folge hat, und die Nutzenden können zusätzlich Einfluss auf die angezeigten Projekte nehmen, sofern dies gewünscht ist.

Hat eine Lyncronize nutzende Person sodann ein passendes Projekt gefunden, so kann sie sich entweder per E-Mail oder direkt über die Plattform auf das jeweilige Projekt bewerben. In unserem Szenario nutzt die Person die Bewerbungsmöglichkeit über die Plattform. Über den Button „Mit Lyncronize bewerben“ erschien bisher ein Fenster, welches die Wahl zwischen „Mit komplettem Profil bewerben“ oder „Profil anpassen“ ließ. Dabei wurde auch die Vollständigkeit des Profils in Prozent angegeben (Feedback Nudge). Innerhalb des Fensters hatten die nutzenden Personen die Möglichkeit, einzelne Angaben im Profil freizugeben oder für den Bewerbungsprozess herauszunehmen. Bisher war hierbei für die Nutzenden allerdings nicht ohne weiteres erkenntlich, welche Informationen zwingend sind und welche Informationen für den konkreten Bewerbungsprozess keine Relevanz entfalten. Um dieses Problem zu lösen, wurden im Projekt Privacy Nudges entwickelt, welche die Nutzenden genau in diesem Punkt unterstützen sollen. Der erste Nudge dient dabei als eine Art Gate-Keeper, welcher einen zusätzlichen Hinweis einbaut, bevor einfach alle Daten herausgegeben werden. Sofern die nutzende Person nunmehr auf den Button „Mit Lyncronize bewerben“ klickt, eröffnet sich eine weitere Möglichkeit. Die Person kann sich nicht mehr nur mit allen Informationen des Profils bewerben oder manuell eine Anpassung vornehmen, sondern es gibt zusätzlich die Option „Bewerben mit besonderem Augenmerk auf meine Daten“ (Privacy Nudge). Lyncronize trifft dabei eine Vorauswahl

an Daten, welche nach den Erfahrungen der Plattform relevant und hilfreich sind und verbirgt automatisch überflüssige Daten. Dadurch werden einerseits nur notwendige Daten preisgegeben, andererseits reduziert es die Bewerbung auch auf wesentliche Punkte und ermöglicht so einen schnellen Überblick für die Unternehmen, die das Projekt ausgeschrieben haben. Somit werden die Interessen sowohl erfahrener als auch unerfahrener Personen berücksichtigt. Der Button „Bewerben mit besonderem Augenmerk auf meine Daten“ wird darüber hinaus grün markiert (Farbelement), um die Aufmerksamkeit auf das Element zu lenken, und mit einem Schloss-Icon (Gütesiegel) versehen, welches die „sichere Alternative“ symbolisieren soll. Zudem wird diese Option durch den Slogan „pre-selected by Lyncronize“ gekennzeichnet. Für den Nutzenden ist somit ersichtlich, wer für die Entscheidungsarchitektur verantwortlich ist und hier den Nudge platziert und sendet. Dies soll die Transparenz der Entscheidungsarchitektur und damit die Autonomie der Nutzenden fördern.

Die Wahrscheinlichkeit einer Verletzung der Privatsphäre ist häufig für Individuen nicht nachvollziehbar und wird folglich oft unterschätzt. Dies ist auch in dieser Situation der Fall. Das Individuum tendiert so dazu, am Arbeitsplatz oder in der Bewerbungsphase risikoreiche Entscheidungen in Bezug auf den Schutz der eigenen Privatsphäre zu treffen. Dies lässt sich unter anderem auf die Repräsentationsheuristik zurückführen, bei der Individuen dazu tendieren, die Häufigkeit der Beobachtungen eines Ereignisses fälschlicherweise mit dessen Eintrittswahrscheinlichkeit in Verbindung zu bringen. Auch die Verfügbarkeitsheuristik spielt hierbei eine große Rolle, bei der Entscheidungen auf Informationen begründet werden, die mental leicht verfügbar sind. Um diesen Heuristiken entgegenzuwirken, wird das Individuum mit einer Information über Risiken und Konsequenzen seines Handelns aufgeklärt. Basierend auf diesen Informationen kann das Individuum eine fundierte Entscheidung in Bezug auf die eigene Privatsphäre treffen. Die Ansprache für die Information soll außerdem personalisiert erfolgen (Personalisierung). Dies soll eine persönliche Beziehung widerspiegeln.

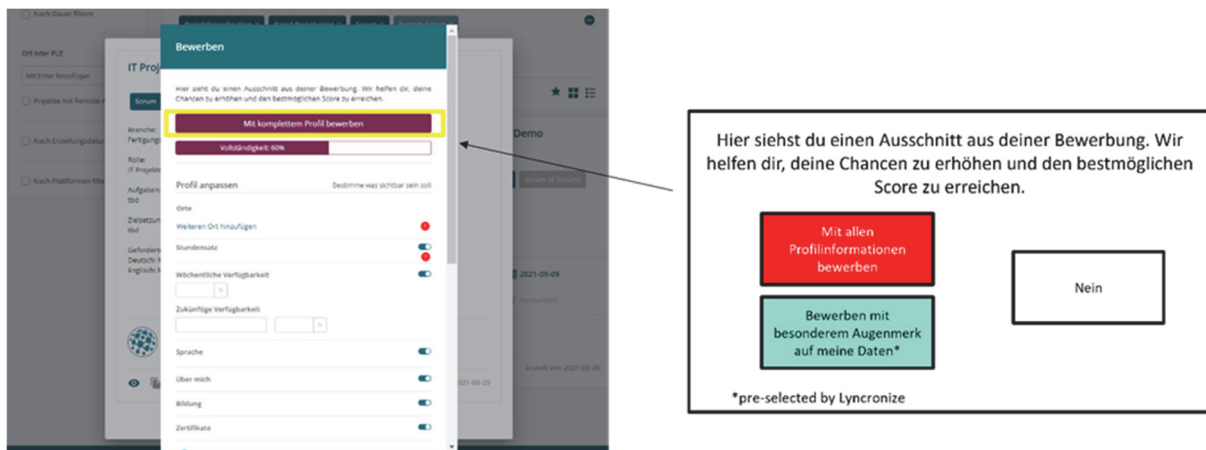


Abbildung 4: Eigene Darstellung. Anwendungsszenario

Das Szenario enthält also einen Feedback Nudge zur Vollständigkeit des Profils und einen Privacy Nudge, welcher wiederum verschiedene Nudge Design Prinzipien bündelt (Gütesiegel, Farbelement, Information und Personalisierung).

8 Evaluation

8.1 Intention

Die Grundintention des Nudges ist es, Nutzenden einer digitalen Plattform für die Vermittlung von Jobs in der IT-Branche zu einem bewussteren beziehungsweise sparsameren Umgang mit ihren persönlichen Daten zu verleiten. Dies geschieht vor dem Hintergrund, dass viele Nutzende dazu neigen, umfängliche Daten zu ihren Qualifikationen und beruflichen Werdegang zu veröffentlichen. Dies geschieht selbst dann, wenn diese Informationen für den Bewerbungserfolg nicht zielführend sind. Für viele Bewerbungsprozesse ist es etwa hinreichend, wenn nur neuere Projekte oder nur für die ausgeschriebene Stelle relevante Kompetenzen aufgelistet werden. Hinsichtlich des Bewusstseins für privatheitsbezogene Risiken gibt es weiterhin bei der digitalen Plattform eine beachtliche Streuung. Einige Nutzende bewegen sich sehr routiniert im digitalen Bereich und geben nur notwendige Informationen preis, wohingegen speziell unerfahrene Nutzende erhebliche kognitive Kapazitäten benötigen, um eine gezielte Auswahl hinsichtlich der Informationen treffen zu können.

Gleichzeitig ist jedoch nicht bekannt, inwieweit Nutzende durch besonders detaillierte Darstellung ihrer beruflichen Laufbahn Risiken eingehen, welche entweder ihren beruflichen Erfolg (niedrigere Vermittlungsquote oder niedrigere Gehälter) oder die persönliche Privatsphäre gefährden. Es wird daher an späterer Stelle dafür argumentiert, dass für einen moralisch gerechtfertigten Einsatz von Privacy Nudges Nutzende Transparenz hinsichtlich der (statischen) Relation zwischen der Menge von geteilten Informationen und den erwartbaren Erfolgchancen in Bewerbungsprozessen erforderlich ist.

Davon ungeachtet zeigt sich, dass der intendierte Privacy Nudge neben dem Schutz der persönlichen Privatsphäre auch eine instrumentelle Rolle erfüllt, insofern der Nudge auch den Bewerbungserfolg erhöhen soll. Hinsichtlich des Schutzes der Privatsphäre ist seitens des Betreibenden der Digitalen Plattform eine genauere Beschreibung möglicher Risiken für Nutzende erforderlich, um ein klareres Bild von der moralischen Legitimität der geplanten Intervention gewinnen zu können. Um dies mit einem Beispiel zu verdeutlichen: es mag ungeschickt für Nutzende mit langjähriger Erfahrung in der IT-Branche sein, sämtliche Qualifikationen und berufliche Projekte anzuführen, hieraus folgt jedoch nicht notwendigerweise, dass das Teilen dieser Informationen berufliche oder private Nachteile bedeutet – von Sonderfällen abgesehen.

8.2 Mechanismen

Hinsichtlich der Mechanismen des Privacy Nudges soll insbesondere durch Gütesiegel oder Farbelemente den Nutzenden signalisiert werden, welche Einstellungen datensparsam oder risikoarm sind. Die Farbelemente haben daneben noch die Funktion, die Aufmerksamkeit der Nutzenden gezielt zu lenken. In diesem Sinne könnten integrale Felder mit grünen Farbelementen untermalt werden, wohingegen nicht-essenzielle Felder gelbe oder rote Farbelemente erhalten.

Sowohl die Gütesiegel als auch die Farbelemente zeichnen sich durch ein hohes Maß an Vertrautheit aus, da sie etwa im Straßenverkehr wohl vertraut sind. Erneut ist aber hervorzuheben, dass transparent gemacht werden sollte, weshalb bestimmte Felder mit den jeweiligen Farbelementen verknüpft werden. Ebenso ist zu hinterfragen, inwieweit es überhaupt Felder bedarf, welche als nicht

hinreichend zielführend oder vertrauenswürdig anzusehen sind. In diesem Sinne gilt es zu hinterfragen, ob es nicht eine elegantere Alternative zu Privacy Nudges sein könnte, von vornherein nur solche Informationen abzufragen, die als bedeutsam gelten.

Ein weiteres Ziel der Privacy-Nudges besteht darin, Nutzende nicht nur dazu zu verleiten, privatheits-sensitive Einstellungen zu wählen, sondern ihr Bewusstsein für die zugrundeliegende Problematik zu schärfen. Demgegenüber ist es eines der Ziele des Privacy-Nudgings Nutzende über die entsprechenden Risiken aufzuklären. Dies ist sicherlich aus ethischer Perspektive als positiv anzusehen, da es der Rationalität und Autonomie von Nutzenden zuträglich ist. Es bleibt bis dato allerdings ungeklärt, wie diese Informationen bereitgestellt werden können.

Hier ergibt sich auch ein konzeptuelles Problem: Nudges unterlaufen eigentlich das deliberative Vermögen von Personen. Versteht die entsprechende Person die zugrunde liegenden Mechanismen, so sollte sich die Wirkung des Nudges abschwächen. Von daher kann die Bereitstellung von Informationen nicht Teil des Privacy Nudges sein, sondern sie muss zusätzlich zum Nudge erfolgen. Eine Option wären hier etwa kurze Erklärvideos, interaktive Formate oder leicht verständliche Texte, bei denen speziell neue Nutzende ermuntert werden könnten, sie sich anzuschauen. In jedem Fall gilt, dass eine Spezifizierung der Transparenzbedingungen ein wichtiges Desiderat für die Implementierung des Privacy Nudges darstellt.

Eine letzte wichtige Komponente des Privacy Nudges ist die Personalisierung des Nudge-Designs. Dies soll mittels einer namentlichen Ansprache der Nutzenden erfolgen. Während es sich hier um eine vermeintlich schwache Form der Personalisierung handelt, sind sicherlich auch stärker personalisierte Informationen denkbar, etwa eine stärkere Anpassung der Sprache an die Präferenzen der Nutzenden. Personalisierte Nudges haben aus ethischer Sicht die Schwierigkeit, die Widerstehbarkeit von Nudges zu gewährleisten. Diese Problematik wurde bereits im Kontext von Hypernudges angesprochen. Je stärker ein Nudge auf das Persönlichkeitsprofil von Nutzenden zugeschnitten wird, desto herausfordernder wird es für die betreffende Person, ihm zu widerstehen. Im schlimmsten Fall konterkariert Personalisierung die Grundidee von Nudges. Diese Bedenken treffen sicherlich nicht auf den für das Projekt relevanten Privacy Nudge zu, da hier weder die Personalisierung besonders tiefgreifend noch die Widerstehbarkeit als eklatant gefährdet anzusehen sind. Es ist aber dennoch wichtig, bei etwaigen Weiterentwicklungen des Privacy Nudges diese Grundproblematik zu bedenken.

8.3 Ethische Bewertung

Im Folgenden soll der Privacy Nudge noch einmal systematisch unter ethischen Gesichtspunkten evaluiert werden. Basierend auf dem ethisch-rechtlichen Vergleich zum Nudging hat sich herauskristallisiert, dass es sich beim Nudging um eine spezifische Art einer paternalistischen Intervention handelt, deren ethische Bewertung sich vornehmlich an drei Eckpfeilern orientiert: dem Respekt vor der Autonomie von Personen, der Widerstehbarkeit von Nudges und der Transparenz hinsichtlich der manipulierten Entscheidungsarchitektur (Schmidt and Engelen 2020).

Die Autonomie von Nutzenden wird im geplanten Privacy Nudge hinreichend respektiert, indem auf Dark-Pattern Designs oder andere übermäßig manipulative Mechanismen verzichtet wird. Aus dem gleichen Grund ist auch eine Widerstehbarkeit des Nudges gewährleistet. Gegeben dem Fall, dass Nutzende hinreichend gut bezüglich der Wirkweise und Mechanismen des Nudges informiert werden, ist nicht zu sehen, inwieweit dieser noch als übermäßig manipulativ zu erachten ist.

Komplizierter sieht es jedoch hinsichtlich der Transparenzbedingungen aus. Einerseits ist nicht klar, inwiefern Nutzende darüber informiert werden sollen, dass sie genudgt werden. Eine Minimalbedingung zur Gewährleistung der Transparenzbedingung wäre hier ein leicht auffindbares Feld, welches – vergleichbar mit der informierten Einwilligung in der Medizin – umfassende Informationen zur Struktur, zur Wirkweise und zu den Risiken des Nudges bereitstellt. Insbesondere sind genauere Erklärungen hinsichtlich der Ziele des Nudges sowie der mit dem Nudge einhergehenden Risiken notwendig. Zwei Aspekte, die hier genauer erläutert werden müssen, sind mögliche Nachteile, welche Nutzende durch datensparsame Einstellungen in Kauf nehmen müssen (für bestimmte Jobs oder Firmen könnte es etwa zielführender sein, ausführliche Informationen bereit zu stellen), sowie generelle Risiken, welche aus dem Teilen von Informationen resultieren.

Möchten die Nutzenden über die Minimalbedingungen hinaus gehen, bieten sich etwa Erklärvideos an. Andererseits besteht das Problem, dass ausgehend von der Beschreibung des Nudges noch nicht hinreichend ersichtlich ist, wie die Nutzenden mittelfristig zu privatheits-sensitiveren Einstellungen erzogen werden sollen.

Ein weiteres ethisches Problem ergibt sich daraus, dass die Nutzenden durch ein Unternehmen genudgt werden sollen. Vor dem Hintergrund, dass die ethischen Risiken des Teilens von Daten in Bewerbungsprozessen nicht hinreichend spezifiziert wurden, ist davon auszugehen, dass eine gemischte Motivation hinsichtlich des Privacy Nudges vorliegt: der Nudge soll zum einen die Privatsphäre von Nutzenden schützen, zum anderen soll er effizientere Bewerbungsprozesse ermöglichen. Der letztgenannte Aspekt birgt vorrangig für den Betreiber der Digitalen Plattform (in dem Fall Lyncronize) Vorteile und kann daher nicht zur ethischen Rechtfertigung herangezogen werden.

8.4 Rechtswissenschaft

Zunächst ist festzuhalten, dass der zu prüfende Privacy Nudge zwar eine Datenverarbeitung auslöst, aber diese nicht selbst durchführt. Die zusätzliche Option der Bewerbung mit durch Lyncronize vorausgewählten Angaben besteht in diesem Szenario von vornherein. Es handelt sich lediglich um ein zusätzliches Fenster und eine Anpassung der Benutzeroberfläche (Farbelement, Gütesiegel und zusätzliche Information), damit die Aufmerksamkeit der Nutzenden auf diese Option gelenkt wird.

Sofern der Nudge selbst keine Daten verarbeitet, richtet sich die datenschutzrechtliche Zulässigkeit des Nudges nach der des Systems, in welches er integriert ist (Grafenstein et al. 2018). Es müssen insbesondere die Anforderungen der DSGVO eingehalten werden. Hier sind die Datenschutzgrundsätze gemäß Art. 5 DSGVO und die Anforderungen an den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO besonders relevant. Privacy Nudges können generell dabei helfen, den abstrakten Art. 25 DSGVO mit Leben zu füllen und die Anforderungen der DSGVO umzusetzen (Schomberg et al. 2019). Die praktische, datenschutzrechtliche Prüfung der Plattform Lyncronize war allerdings nicht Gegenstand des Projektes. Das Start-Up Lyncronize beschäftigt dafür einen externen Datenschutzbeauftragten, welcher für die praktische Umsetzung der Anforderungen der DSGVO zuständig und verantwortlich ist. In Ermangelung widerstreitender Informationen ist daher von der DSGVO-Konformität der Plattform Lyncronize auszugehen. Daher stellt sich hier lediglich die Frage, ob einzelne der genannten Design Elemente des Privacy Nudges die Datenschutzkonformität des Systems negativ beeinflussen.

Bei dem Gütesiegel und Farbelement des Privacy Nudges handelt es sich um Anpassungen der Benutzeroberfläche. Was das Design von Benutzeroberflächen angeht, gibt es kaum Regulierung, da es zunächst jedem Anbietenden freisteht, diese kreativ zu gestalten. Art. 25 DSGVO macht jedoch einige Angaben zur Technikgestaltung, welche sich auch auf die Benutzeroberfläche beziehen kann (Loy and Baumgartner 2021). Art. 25 DSGVO wiederum verweist auf die Datenschutzgrundsätze in Art. 5 DSGVO. Die datenschutzfreundliche Gestaltung der Benutzeroberfläche muss daher, unter anderem, auch den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und den der Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a 2. Alt. DSGVO) berücksichtigen. Der Grundsatz der Datenverarbeitung nach Treu und Glauben ist dabei nicht mit dem Rechtsgrundsatz Treu und Glauben des § 242 BGB gleichzusetzen. Es handelt sich eher um eine unglückliche Übersetzung. Gemeint ist die Möglichkeit, eine formal rechtmäßige Datenverarbeitung als rechtswidrig qualifizieren zu können, wenn dadurch Vertrauen missbraucht wird oder die Verarbeitung generell unfair ist. Der in der englischen Fassung verwendete Begriff „fairness“ wäre daher auch in der deutschen Fassung treffender und wird teilweise auch in der deutschen Literatur verwendet (Roßnagel 2018). Das Design darf also nicht dazu verleiten, mehr Daten preiszugeben als notwendig. Die hier vorgenommenen Änderungen in der Benutzeroberfläche sollen die Nutzenden jedoch eher zu einer datenschutzfreundlicheren Nutzung bewegen. Sie stehen daher nicht im Widerstreit mit dem Grundsatz der Datenminimierung. Der Grundsatz der Fairness gebietet es generell, dass Heuristiken und Biases der Nutzenden nicht trickreich ausgenutzt werden. Es könnte darüber nachgedacht werden, ob das Farbelement Mechanismen der Nutzenden ausnutzt und somit ein Verstoß gegen den Grundsatz der Fairness vorliegen könnte. Das Farbelement kann zwar die Aufmerksamkeit auf die datenschutzfreundlichere Lösung lenken, aber daneben gibt es noch ein gleich großes Kästchen mit anderen Optionen. Es wird also keine Option versteckt. Auch wird ausdrücklich darauf hingewiesen, dass es sich um eine Auswahl von Lyncronize handelt. Dadurch, dass die Nutzenden so wissen, wer die Vorauswahl getroffen hat, können sie bei ihrer Abwägung einbeziehen, wie die Interessen von Lyncronize gelagert sein könnten. Das der Fokus hier auf die datenschutzfreundliche Option gelenkt wird, stimmt außerdem mit dem Sinn und Zweck des Art. 25 DSGVO überein.

Auch das Design Element der Information des Privacy Nudges beeinflusst die Datenschutzkonformität von Lyncronize nicht negativ. Die DSGVO schreibt sogar Informationspflichten (insbesondere Art. 12, 13 und 14 DSGVO) und Transparenz (Art. 5 Abs. 1 lit. a 3. Alt. DSGVO) vor. Auch wenn im Einzelnen stark umstritten ist, wie diese umgesetzt werden sollten (Geminn et al. 2021), so ist zumindest ein übersichtlicher, klar formulierter Hinweis, wie er im Demonstrator vorgesehen ist, kein Hindernis.

Die personalisierte Ansprache als Design Element könnte hingegen selbst personenbezogene Daten, nämlich den Namen, verarbeiten. Auch bei dem Feedback Nudge über die Vollständigkeit des Profils hat sich aus der Beschreibung nicht ergeben, ob dieser selbstständig Daten verarbeitet. Die Möglichkeit besteht. Dann müssten das personalisierte Element im Privacy Nudge und der Feedback Nudge selbst am Maßstab der DSGVO gemessen werden. Dabei handelt es sich jedoch eher um eine Formalität, da der Maßstab identisch bleibt. Zumindest finden diese Verarbeitungen innerhalb des übergeordneten Systems statt, weswegen sich auch die Rechtsgrundlage der Datenverarbeitung im System auf diese Verarbeitungen erstrecken dürfte. Auch hier ist also vor allem zu prüfen, ob die Elemente mit Art. 25 DSGVO vereinbar sind.

Wie bereits im Rahmen der ethischen Bewertung erwähnt, handelt es sich bei der personalisierten Ansprache um eine schwache Form der Personalisierung. Dadurch kann gegebenenfalls eine etwas persönlichere Beziehung zum System aufgebaut und etwas mehr Vertrautheit geschaffen werden,

aber die Widerstehbarkeit ist noch gegeben. Außerdem soll die personalisierte Ansprache hier den Privacy Nudge unterstützen, welcher wiederum zur Datenminimierung beitragen soll und damit im Einklang mit Art. 25 Abs. 1 DSGVO ist.

Etwas problematischer könnte lediglich der Feedback Nudge sein, da sich Lyncronize nutzende Personen durch die Angabe der Vollständigkeit des Profils dazu verleitet fühlen könnten, 100 % zu erreichen. Wenn eine Person also bisher nur 70 % des Profils ausgefüllt hat und diese Rückmeldung bekommt, so könnte sich die Person dadurch dazu aufgefordert fühlen, 100 % zu erreichen, obwohl die 70 % vielleicht schon völlig ausreichend sind, um sich aussichtsreich auf ein vorgeschlagenes Projekt zu bewerben. Allerdings sind die Profile bei Lyncronize nicht automatisch für eine Vielzahl von Personen freigegeben. Es ist viel eher so, dass nur Nutzende ihre eigenen Profile sehen können, bis sie sich auf bestimmte Projekte bewerben. Und bevor die Daten für diesen Schritt freigegeben werden, kommt der Privacy Nudge zum Einsatz und es wird darauf hingewirkt nur notwendige Daten zu teilen.

Zuletzt lässt sich generell die Frage stellen, ob das Nudging im Demonstrator nicht vielleicht schon deshalb illegitim ist, weil es doch eher paternalistisch als libertär ist. Allerdings ist, wie bereits erwähnt, nur der Staat direkt an Grundrechte, und somit auch an den aus dem Rechtsstaatsprinzip erwachsenen Grundsatz der Verhältnismäßigkeit, gebunden. Private sind nur mittelbar an Grundrechte gebunden, weswegen die generellen Bedenken im privatrechtlichen Bereich abgemildert sein dürften. Außerdem ist schon staatlicher Paternalismus zu rechtfertigen, wenn es dem Gemeinwohl dient. Das müsste dann erst recht im Bereich Privater gelten. Datenschutz als Ausprägung des Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hat auch eine Gemeinwohlkomponente, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit der Menschen begründeten freiheitlich demokratischen Gemeinwesens ist. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffen Informationen, zum Beispiel im Arbeitsumfeld bekannt sind, kann in seiner Freiheit selbstbestimmt zu entscheiden gehemmt sein (BVerfGE 65, 1 (43)).

Falls Arbeitgebende, und nicht wie hier Dritte (Lyncronize), einen solchen Privacy Nudge in ihr online Bewerbungsportal integrieren würden, so käme ein weiteres Argument zur Rechtfertigung hinzu: Arbeitgebende haben gegenüber Arbeitnehmenden Schutzpflichten. Gemäß § 26 BDSG zählen auch Bewerbende im Bereich des Beschäftigtendatenschutzes bereits als Arbeitnehmende und sind daher vom Schutz umfasst.

Natürlich unterliegen auch Entscheidungsbeeinflussende, in diesem Fall Lyncronize oder Arbeitgebende, immer Heuristiken und Biases. Aber der hier vorgeschlagene Privacy Nudge wurde nicht ausschließlich danach entwickelt, was Lyncronize für richtig hält oder was wir im Projekt für richtig halten, sondern Orientierung hat hier die DSGVO und insbesondere Art. 25 DSGVO geboten. Die DSGVO ist als Verordnung wiederum demokratisch legitimiert. Es werden also die Regelungen umgesetzt, die wir uns als Gesellschaft gegeben haben und nicht die, die nur das Projektkonsortium für richtig befindet.

Der Feedback Nudge und der Privacy Nudge sind daher rechtmäßig. Vor allem der Privacy Nudge ist vor dem Hintergrund der DSGVO sogar besonders begrüßenswert.

9 Empfehlungen

Nach eingehender Betrachtung bestehen keine ernsthaften Bedenken hinsichtlich der moralischen Legitimität des Privacy Nudgings im Demonstrator. Es gilt jedoch zu bedenken, dass wir es hier mit einem Demonstrator zu tun haben und sobald subtilere/technisch ausgeklügeltere Mechanismen benutzt werden, eine Neubetrachtung vonnöten ist (Yeung 2017).

Beim Design von Benutzeroberflächen sollte jedoch stets bedacht werden, wie die Nutzenden durch das Design gelenkt werden könnten. In Art. 25 DSGVO sind schon längst bußgeldbewehrte Angaben zum Design der Technik und damit auch zum Design der Benutzeroberfläche enthalten, diese werden jedoch noch nicht konsequent genug umgesetzt (Loy and Baumgartner 2021). Über das durch Art. 25 DSGVO notwendige Maß hinaus, welches auf Grund der Abstraktheit der Norm nicht einfach zu bestimmen ist, können Verantwortliche jedoch stets versuchen, ein möglichst datenschutzfreundliches Design zu wählen.

Privacy Nudges können ein geeignetes Tool sein, um ein an sich schon datenschutzkonformes System noch datenschutzfreundlicher zu gestalten. Technische Systeme könnten so rechtsverträglich werden. Das Konzept der Rechtsverträglichkeit hat das Ziel, nicht das kurzfristige Minimum, sondern das langfristige Optimum an Grundrechtsschutz zu gewährleisten (Thies et al. 2020). Das ursprünglich verfassungsrechtliche Konzept wurde weiterentwickelt und auf alle Rechtsnormen erstreckt (Roßnagel 1993). Um Technik rechtsverträglich zu gestalten, werden dazu die relevanten rechtlichen Rahmenbedingungen (hier insbesondere Art. 25 DSGVO) analysiert und vorausschauend in die Systementwicklung integriert. Das Konzept der Rechtsverträglichkeit berücksichtigt dabei die Veränderung der Rechtsordnung in der Zukunft am Maßstab heutiger Rechtsziele (Roßnagel 1993). Die einzelnen Rechtsnormen sind dabei in ihrer Funktion als Kriterien für die Technik(folgen)bewertung als Optimierungsaufträge zu verstehen. Es soll also keine Aussage getroffen werden, ob die rechtlichen Anforderungen der Norm erfüllt oder nicht erfüllt sind. Stattdessen es wird danach gefragt, ob eine Entwicklung die Erreichung des Ziels, also die in unseren Rechtsnormen beschriebene Gesellschaftsordnung, unterstützt oder fördert. Sofern dies der Fall ist, ist die Entwicklung rechtsverträglich. Eine Entwicklung, die die Erreichung des Ziels hingegen erschwert oder gar verhindert verträgt sich gerade nicht mit dem Ziel und ist daher auch nicht rechtsverträglich (Roßnagel 1993). Das Konzept berücksichtigt die Veränderung der Rechtsordnung in der Zukunft. Rechtsverträglichkeit ist daher nicht mit Rechtmäßigkeit gleichzusetzen, da diese Bewertung bezogen auf einen Sachverhalt nur so lange Gültigkeit hat, wie dieser unverändert bleibt. Aus diesem Grund ist Rechtsverträglichkeit auch nicht das Gegenteil von Rechtswidrigkeit (Roßnagel 1993).

Nach dem Maßstab heutiger Rechtsziele von Art. 25 DSGVO sollen technische Systeme datenschutzfreundlich gestaltet werden, was unter anderem umfasst, dass nur notwendige Daten verarbeitet werden. Dies dient letzten Endes auch dem Schutz der informationellen Selbstbestimmung, welche eine Bedingung für unsere Gesellschaft ist, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlung- und Mitwirkungsfähigkeit seiner Bürgerinnen und Bürger begründeten freiheitlich demokratischen Gemeinwesens ist (BVerfGE 65, 1 (43)). Sofern die Privacy Nudges im Demonstrator also dazu führen sollen, dass die Nutzenden nicht alle, sondern nur alle notwendigen Daten preisgeben, unterstützen die Nudges das hier relevante Rechtsziel. Privacy Nudges können also ein Tool sein, um zu einer datenschutzrechtlich rechtsverträglichen Gestaltung zu gelangen. Ähnlich wie bei der Umsetzung des Art. 25 DSGVO (Schomberg et al. 2019), müssen jedoch stets weitere Maßnahmen hinzukommen.

10 Fazit

Generelle Kritik gegenüber Privacy Nudging ist nicht vollständig von der Hand zu weisen – letztlich unterliegen immer auch die Entscheidungsbeeinflussende Biases und Heuristiken. Diese Bedenken lassen sich jedoch auf ein absolutes Minimum reduzieren, wenn Privacy Nudging geleitet durch gesetzliche Vorgaben und dadurch demokratisch legitimiert stattfindet.

Mit dem entwickelten Designtool, wie der Methode und den Entwurfsmustern wird ein Beitrag zu Theorie und Praxis geleistet. Durch die Entwurfsmuster wird Designwissen kodifiziert und den Nutzenden zugänglich gemacht. In Bezug auf das DELEN Model wurde ein digitales Nudging-Prozessmodell entwickelt, das eine legitime und effektive Gestaltung und Entwicklung digitaler Nudges fördert. Es wird eine systematische Anleitung für die Entwicklung von digitalen Nudges geboten, die ethische, rechtliche, psychologische und gesellschaftlich-normative Randbedingungen erfüllen.

Die Designtools sind komprimiert und formalisiert, um Entscheidungsbeeinflussende leicht verständliches und zugängliches Wissen über die Gestaltung digitaler Nudges, die wichtige rechtliche und ethische Standards erfüllen, bereitzustellen. Es werden normative Grenzen als integrale Elemente in beispielsweise dem Modell implementiert, um eine Zielgruppensegmentierung als Schlüsselement vorgeschlagen. Diese erhöht die Wirksamkeit von Nudges und vermeidet unnötige Belastungen für andere Individuen. Auf diese Weise ebnet das Modell den Weg für legitime und effektivere digitale Nudges. Durch die Anwendung können Entscheidungsbeeinflussende Nudge-Designs leichter vergleichen und verbessern.

Selbst wenn digitale Nudges scheitern, können die Entscheidungsbeeinflussende systematisch alle Elemente des systematischen Modells durchgehen und ihre Ausführung bewerten. Auch wenn unser digitales Nudge-Modell Richtlinien in einer digitalen Umgebung bietet, ist die Übertragung in eine reale Umgebung zu testen. Dieses Modell an reale Umgebungen anzupassen, könnte ein erfolgreiches Unterfangen für die Zukunft sein.

11 Literaturverzeichnis

- Acquisti, A. 2009. "Nudging Privacy: The Behavioral Economics of Personal Information," *IEEE Security & Privacy Magazine* (7:6), pp. 82-85 (doi: 10.1109/MSP.2009.163).
- Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., and Schaub, F. 2017. "Nudges for Privacy and Security," *ACM Computing Surveys* (50:3), pp. 1-41 (doi: 10.1145/3054926).
- Alavi, M., and Leidner, D. E. 2001. "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues," *MIS Quarterly* (Vol. 25), pp. 107-136.
- Alexander, C. 1977. *A pattern language: towns, buildings, construction*, Oxford University Press.
- Backhaus, N. 2019. "Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz: Ein meta-analytisches Review zur Auswirkung elektronischer Überwachung auf Beschäftigte," *Zeitschrift für Arbeitswissenschaft* (73:1), pp. 2-22 (doi: 10.1007/s41449-018-00140-z).
- Bakshy, E., D. Eckles, R. Yan, and I. Rosenn. 2012. *Social influence in social advertising: evidence from field experiments*, ACM.
- Barev, T. J., Schöbel, S., Janson, A., and Leimeister, J. M. 2021. "DELEN – A Process Model for the Systematic Development of Legitimate Digital Nudges," in *The Next Wave of Sociotechnical Design*, L. Chandra Kruse, S. Seidel and G. I. Hausvik (eds.), Cham. 2021, Cham: Springer International Publishing, pp. 299-312.
- Barth, S., and Jong, M. D. de. 2017. "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," *Telematics and Informatics* (34:7), pp. 1038-1058 (doi: 10.1016/j.tele.2017.04.013).
- Belanger, F., and Hiller, J. S. 2006. "A framework for e-government: privacy implications," *Business Process Management Journal* (12:1), pp. 48-60.
- Bélanger, and Crossler. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), p. 1017 (doi: 10.2307/41409971).
- Chang, D., Krupka, E. L., Adar, E., and Acquisti, A. "Engineering Information Disclosure," in *CHI'16 Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 587-597 (doi: 10.1145/2858036.2858346).
- Coventry, L. M., Jeske, D., Blythe, J. M., Turland, J., and Briggs, P. 2016. "Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance," *Frontiers in psychology* (7), p. 1341 (doi: 10.3389/fpsyg.2016.01341).
- Dalecke, S., and Karlsen, R. 2020. "Designing Dynamic and Personalized Nudges," in *Proceedings of 10th International Conference on Web Intelligence, Mining and Semantics (WIMS 2020) & 5th International Conference on Real-time Intelligent Systems (RTIS 2020) : 30 June – 3 July 2020, Biarritz, France*, R. Chbeir, Y. Manolopoulos, R. Akerkar and J. Mizera-Pietraszko (eds.), Biarritz France. 30 06 2020 03 07 2020, New York, New York: Association for Computing Machinery, pp. 139-148 (doi: 10.1145/3405962.3405975).
- Eigenbrod, L., and Janson, A. 2018. *How digital nudges influence consumers—experimental investigation in the context of retargeting*.
- Erevelles, S., Fukawa, N., and Swayne, L. 2016. "Big Data consumer analytics and the transformation of marketing," *Journal of Business Research* (69:2), pp. 897-904 (doi: 10.1016/j.jbusres.2015.07.001).
- Faraj, S., and Sproull, L. 2000. "Coordinating Expertise in Software Development Teams," *Management Science* (46:12), pp. 1554-1568.
- Ferreira, N., Aïmeur, E., Hage, H., Heisel, M., and van Hoogstraten, C. 2020 - 2020. "Persuasion Meets AI: Ethical Considerations for the Design of Social Engineering Countermeasures," in *Proceedings of the 12th International Joint Conference on Knowledge Discovery, Knowledge*

- Engineering and Knowledge Management*, Budapest, Hungary. 11/2/2020 - 11/4/2020, SCITEPRESS - Science and Technology Publications, pp. 204-211 (doi: 10.5220/0010142402040211).
- Gamma, E. 1995. "Design patterns: elements of reusable object-oriented software," *Pearson Education India*.
- Geminn, C., Francis, L., and Herder, K.-R. 2021. "Die Informationspräsentation im Datenschutzrecht - Auf der Suche nach Lösungen. In: Newsdienst der Zeitschrift für Datenschutz (ZD-Aktuell), 05335."
- Gerg, S. 2019. *Nudging: Verfassungsrechtliche Maßstäbe für das hoheitliche Einwirken auf die innere Autonomie des Bürgers*.
- Grafenstein, M. von, Hölzel, J., Irgmaier, F., and Pohle, J. 2018. *Nudging – Regulierung durch Big Data und Verhaltenswissenschaften*.
- Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), pp. 611-642.
- Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS Quarterly* (37:2), pp. 337-355.
- Gregor, S., and Jones, D. 2007. "The Anatomy of a Design Theory," *Association for Information Systems* (8:5), pp. 1-60.
- Hertwig, R., and Grüne-Yanoff, T. 2017. "Nudging and Boosting: Steering or Empowering Good Decisions," *Perspectives on psychological science : a journal of the Association for Psychological Science* (12:6), pp. 973-986 (doi: 10.1177/1745691617702496).
- Ho, S. Y., and Lim, K. H. 2018. "Nudging Moods to Induce Unplanned Purchases in Imperfect Mobile Personalization Contexts," *MIS Quarterly* (42:3), pp. 757-778 (doi: 10.25300/MISQ/2018/14083).
- Hummel, D., and Maedche, A. 2019. "How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies," *Journal of Behavioral and Experimental Economics* (80), pp. 47-58 (doi: 10.1016/j.socec.2019.03.005).
- Indulska, M., Green, P., Recker, J., and Rosemann, M. 2009. "Business Process Modeling: Perceived Benefits," in *Conceptual Modeling - ER 2009*, A. H. F. Laender, S. Castano, U. Dayal, F. Casati and J. P. M. de Oliveira (eds.), Berlin, Heidelberg. 2009, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 458-471.
- Kahneman, D. 2013. *Thinking, fast and slow (1st pbk. ed.)*, New York: Farrar, Straus and Giroux.
- Khern-am-nuai, W., Yang, W., and Li, N. 2016. "Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment," *SSRN Electronic Journal* (doi: 10.2139/ssrn.2800499).
- Kirchhof, G. 2015. "Nudging - zu den rechtlichen Grenzen informalen Verwaltens," *Zeitschrift für Rechtspolitik* (48:5), pp. 136-137.
- Kort, M. 2017. "Der Beschäftigtendatenschutz gem. § 26 BDSG-neu.,"
- Kort, M. 2018. "Die Bedeutung der neueren arbeitsrechtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes," *17*, pp. 1097-1105.
- Krimphove, D. 2017. "Nudging als Mittel der ergänzenden Verhaltenssteuerung im Rechtssystem?" *Rechtstheorie* (48:3), pp. 299-314 (doi: 10.3790/rth.48.3.299).
- Kroll, T., and Stieglitz, S. 2021. "Digital nudging and privacy: improving decisions about self-disclosure in social networks," *Behaviour & Information Technology* (40:1), pp. 1-19 (doi: 10.1080/0144929X.2019.1584644).
- Krönke, C. 2016. "Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung," *Der Staat* (55:3), pp. 319-351 (doi: 10.3790/staa.55.3.319).
- Laue, P. 2019. "Kremer, S. (Hg.): Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage. Baden-Baden:,"

- Lewinski, K. von. 2020. *Medienrecht: Ein Studienbuch*, München: Verlag C.H.BECK oHG.
- Liu, B., Andersen, M. S., Schaub, F., Almuhiemedi, H., Zhang, S., Sadeh, N., Agarwal, Y., and Acquisti, A. 2005. "Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions," in *Proceedings of the Third International Conference on Mobile Systems, Applications, and Services (MobiSys 2005): June 6 - 8, 2005, Seattle, WA, USA*, Berkley, Calif.: Usenix Association, pp. 27-41.
- Lobo. 2017. "Nudging-Du willst es doch auch. Oder," *Der Spiegel*. Online verfügbar unter <https://www.spiegel.de/netzwelt/web/nudging-sascha-lobo-ueber-das-prinzip-nudging-im-digitalen-zeitalter-a-1172423.html>.
- Loy, C., and Baumgartner, U. 2021. *Consent-Banner und Nudging. Tracking-Mechanismen: Wie viel "Anstupsen" ist erlaubt*.
- Lukyanenko, R., and Parsons, J. 2020. "Design Theory Indeterminacy: What is it, how can it be reduced, and why did the polar bear drown?" *JAIS*, pp. 1-59.
- Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (UIIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355 (doi: 10.1287/isre.1040.0032).
- Martini, M., and Kühling, J. 2016. *Die Datenschutz-Grundverordnung-Revolution oder Evolution im Datenschutzrecht im europäischen und nationalen Datenschutzrecht?*
- McLure-Wasko, M. 1999. "How are Knowledge Management Systems Different from Information Systems, and Who Cares?" *Americas Conference on Information Systems (AMCIS) 1999 Proceedings*, pp. 486-488.
- Meske, C., and Potthoff, T. 2017. *The DINU-model—a process model for the design of nudges*.
- Mirsch, T., Lehrer, C., and Jung, R. 2018. "Making Digital Nudging Applicable: The Digital Nudge Design Method," *Proceedings of the 39th International Conference on Information Systems (ICIS)*.
- Mongin, P., and Cozic, M. 2018. "Rethinking nudge: not one but three concepts," *Behavioural Public Policy* (2:1), pp. 107-124 (doi: 10.1017/bpp.2016.16).
- Müller, R. M., and Thoring, K. 2010. "A Typology of Design Knowledge: A Theoretical Framework," *Americas Conference on Information Systems (AMCIS) Proceedings*.
- Nonaka, I., and Takeuchi, H. 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, Oxford University Press.
- Nonaka, I., and Toyama, R. 2003. "The knowledge-creating theory revisited: knowledge creation as a synthesizing process," *Knowledge Management Research & Practice*, pp. 2-10.
- Peffer, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," *JMIS*, pp. 45-77.
- Roßnagel, A. 1993. "Risikogesellschaft als Informationsgesellschaft," in *Risiken informatisierter Produktion*, VS Verlag für Sozialwissenschaften, Wiesbaden, pp. 19-32 (doi: 10.1007/978-3-322-94237-1_3).
- Roßnagel, A. 2018. *Das neue Datenschutzrecht*.
- Sandfuchs, B., and Kapsner, A. 2018. *Privatheit in der digitalen Gesellschaft*, Berlin: Duncker & Humblot.
- Schmidt, A. T., and Engelen, B. 2020. "The ethics of nudging: An overview," *Philosophy Compass* (15:4), e12658 (doi: 10.1111/phc3.12658).
- Schmidt, B. 2019a. "Kommentierung zu Art. 1 DSGVO. In: Taeger, J; Gabel, D. (Hg.): DSGVO - BDSG - TTDSG Kommentar, 3. Auflage. Frankfurt a. M.: dfv Mediengruppe - Fachmedien Recht und Wissenschaft."
- Schmidt, K. J. 2019b. "Datenschutz und Big Data – Ein Spannungsverhältnis," *Nomos Verlagsgesellschaft mbH & Co. KG*, pp. 265-284 (doi: 10.5771/9783845295183-265).

- Schneider, C., Weinmann, M., and Vom Brocke, J. 2018. "Digital nudging," *Communications of the ACM* (61:7), pp. 67-73 (doi: 10.1145/3213765).
- Schöbel, S., Schomberg, S., Barev, T. J., Grote, T., Janson, A., Hornung, G., and Leimeister, J. M. 2020. "Zum Datenschutz gestupst? Gestaltungsorientierte Entwicklung von Privacy Nudges vor dem Hintergrund ethischer und rechtlicher Leitlinien," 12.11.2020-13.11.2020.
- Schöbel, S. M., Schomberg, S., Barev, T. J., Grote, T., Janson, A., Hornung, G., and Leimeister, J. M. 2022. "Zum Datenschutz gestupst? Gestaltungsorientierte Entwicklung von Privacy Nudges vor dem Hintergrund ethischer und rechtlicher Leitlinien," in *Selbstbestimmung, Privatheit und Datenschutz*, M. Friedewald, M. Kreuzer and M. Hansen (eds.), Wiesbaden: Springer Fachmedien Wiesbaden, pp. 369-388 (doi: 10.1007/978-3-658-33306-5_18).
- Schomberg, S., Barev, T. J., Janson, A., and Hupfeld, F. 2019. "Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging," *Datenschutz und Datensicherheit - DuD* (43:12), pp. 774-780 (doi: 10.1007/s11623-019-1204-5).
- Schomberg, S., Dickhaut, E., Barev, T. J., and Janson, A. 2021. "Mithilfe von Privacy Nudging zu rechtsverträglichen Videokonferenztools,"
- Smith, Dinev, and Xu. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), p. 989 (doi: 10.2307/41409970).
- Spiekermann, S. 2016. *Ethical IT innovation: A value-based system design approach*, Boca Raton, London, New York: CRC Press Taylor & Francis Group.
- Sundar, S. S., Kim, J., Rosson, M. B., and Molina, M. D. 2020. "Online Privacy Heuristics that Predict Information Disclosure," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, R. Bernhaupt, F. ' . Mueller, D. Verweij, J. Andres, J. McGrenere, A. Cockburn, I. Avellino, A. Goguey, P. Bjørn, S. Zhao, B. P. Samson and R. Kocielnik (eds.), Honolulu HI USA. 25 04 2020 30 04 2020, [S.l.]: Association for Computing Machinery, pp. 1-12 (doi: 10.1145/3313831.3376854).
- Sunstein, C. R. 2015. "Do People Like Nudges?" *SSRN Electronic Journal* (doi: 10.2139/ssrn.2604084).
- Sunstein, C. R. 2017. "Nudges that fail," *Behavioural Public Policy* (1:1), pp. 4-25 (doi: 10.1017/bpp.2016.3).
- Sunstein, C. R., and Reisch, L. A. 2013. "Green by Default," *Kyklos* (66:3), pp. 398-402 (doi: 10.1111/kykl.12028).
- Thaler, R. H., and Sunstein, C. R. 2008a. *Nudge: Improving decisions about health, wealth, and happiness*, New York, NY: Penguin.
- Thaler, R. H., and Sunstein, C. R. 2008b. *Nudge: improving decisions about health: A Caravan book large print ed.*, New Haven: Yale University Press.
- Thaler, R. H., and Sunstein, C. R. 2009. *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Penguin Books.
- Thies, L. F., Dickhaut, E., Janson, A., Roßnagel, A., Leimeister, J. M., and Söllner, M. 2020. "Die Simulationsstudie als Evaluationsmethode," *Datenschutz und Datensicherheit - DuD* (44:9), pp. 589-593 (doi: 10.1007/s11623-020-1330-0).
- Turland, J., Coventry, L., Jeske, D., Briggs, P., and van Moorsel, A. 2015. *Nudging towards security: Developing an application for wireless network selection for android phones*, ACM.
- Tversky, A., and Kahneman, D. 1974. "Judgment under un-certainty: Heuristics and biases," *science* (185:4157), pp. 1124-1131.
- van Aken, J. E. 2005. "Valid knowledge for the professional design of large and complex design processes," *Design Studies* (26:4), pp. 379-404 (doi: 10.1016/j.destud.2004.11.004).
- Veil, W. 2018. *The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law*.

- Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., and Cleven, A. 2009. "Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research,"
- Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., and Sadeh, N. 2014. "A field trial of privacy nudges for facebook," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, M. Jones, P. Palanque, A. Schmidt and T. Grossman (eds.), Toronto, Ontario, Canada. 4/26/2014 - 5/1/2014, New York, New York, USA: ACM Press, pp. 2367-2376 (doi: 10.1145/2556288.2557413).
- Weinmann, M., Schneider, C., and Vom Brocke, J. 2016. "Digital Nudging," *Business & Information Systems Engineering* (58:6), pp. 433-436 (doi: 10.1007/s12599-016-0453-1).
- Weinzierl, Q. 2020. *Dark Patterns als Herausforderung für das Recht: Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien.*
- Westin, A. F. 1967. *Special report: legal safeguards to insure privacy in a computer society.*
- Wybitul, T. 2017. *EU-Datenschutz-Grundverordnung: Handbuch*, Fachmedien Recht und Wirtschaft.
- Yeung, K. 2017. "'Hypernudge': Big Data as a mode of regulation by design," *Information, Communication & Society* (20:1), pp. 118-136 (doi: 10.1080/1369118X.2016.1186713).
- Weinzierl, Q. (2020): Dark Patterns als Herausforderung für das Recht – Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien. In: *Neue Zeitschrift für Verwaltungsrecht – Extra* 39 (15), S. 1-11.
- Westin, A. F. (1967): *Privacy and Freedom*. New York: Atheneum.
- Wybitul, T. (2017): Der neue Beschäftigtendatenschutz nach Art. 26 BDSG und Art. 88 DSGVO. In: *Neue Zeitschrift für Arbeitsrecht* 34 (7), S. 413-419.
- Yeung, K. (2017): ‚Hypernudge‘: Big Data as a mode of regulation by design. In: *Information, Communication & Society* 20 (1), S. 118-136.

Publikationsverzeichnis der im Projekt erarbeiteten Forschungspapiere

2023

- Purohit, A.; Barev, T.; Schöbel, S.; Janson, A. & Holzer, A. (2023): Designing for Digital Wellbeing on a Smartphone: Co-creation of Digital Nudges to Mitigate Instagram Overuse. In: Hawaii International Conference on System Sciences (HICSS)

2022

- Dickhaut, E.; Janson, A.; Leimeister, J. M. (2022): Conceptualizing Design Knowledge in IS Research – A Review and Taxonomy of Design Knowledge Properties. Hawaii International Conference on System Sciences (HICSS). Hawaii, USA.
- Schöbel, S.; Schomberg, S.; Barev, T. J.; Grote, T.; Janson, A.; Hornung, G. & Leimeister, J. M. (2022): Zum Datenschutz gestupst? Gestaltungsorientierte Entwicklung von Privacy Nudges vor dem Hintergrund ethischer und rechtlicher Leitlinien. In: Selbstbestimmung, Privatheit und Datenschutz, Wiesbaden.

2021

- Barev, T. J.; Schöbel, S.; Janson, A.; Leimeister, J. M. (2021): DELEN – A Process Model for the Systematic Development of Legitimate Digital Nudges. In: Chandra Kruse, L.; Seidel, S.; Hausvik, G. I. (Hg.) International Conference on Design Science Research in Information Systems and Technology (DESRIST). Cham: Springer. S. 299-312.
- Barev, T. J.; Schwede, M.; Janson, A. (2021): The Dark Side of Privacy Nudging – An Experimental Study in the Context of a Digital Work Environment. Hawaii International Conference on System Sciences (HICSS).
- Schomberg, S.; Dickhaut, E.; Barev, T. J.; Janson, A. (2021): Mithilfe von Privacy Nudging zu rechtsverträglichen Videokonferenztools. In: Informatik 2021 - 51. Jahrestagung der Gesellschaft für Informatik (GI). Kassel, Germany: Gesellschaft für Informatik (GI).
- Benner, D.; Schöbel, S.; Janson, A. (2021): It is only for your own good, or is it? Ethical Considerations for Designing Ethically Conscious Persuasive Information Systems. Americas Conference on Information Systems (AMCIS). Montreal, Kanada.
- Janson, A.; Kreidel, L.; Schöbel, S.; Hornung, G.; Söllner, M.; Leimeister, J. M. (2021): Datenkompetenz durch edukatives Privacy Nudging: Zentrale Prinzipien und Effekte auf Lernprozesse. In: Stapf, I.; Quinn, R. A.; Friedewald, M.; Heesen, J.; Krämer, N. (Hg.): Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zu Privatheit und Datenschutz in Kindheit und Jugend. Baden-Baden: Nomos, S. 255-277.

2020

- Barev, T. J.; Janson, A.; Leimeister, J. M. (2020): Designing Effective Privacy Nudges in Digital Environments: A Design Science Research Approach. International Conference on Design Science Research in Information Systems and Technology (DESRIST). S. 388-393. Springer, Cham.

- Schöbel, S., Janson, A., Jahn, K., Kordyaka, B., Turetken, O., Djafarova, N., Saqr, M., Wu, D., Söllner, M., Adam, M., Heiberg Gad, P., Wesseloh, H., Leimeister, J.M.: A Research Agenda for the Why, What, and How of Gamification Designs Results on an ECIS 2019 Panel. Communications of the Association for Information Systems. (2020).
- Schöbel, S.; Barev, T. J.; Janson, A.; Hupfeld, F.; Leimeister, J. M. (2020): Understanding User Preferences of Digital Privacy Nudges – A Best-Worst Scaling Approach. Hawaii International Conference on System Sciences (HICSS).
- Schöbel, S.; Schomberg, S.; Barev, T. J.; Grote, T.; Janson, A.; Hornung, G.; Leimeister, J. M. (2020): Zum Datenschutz gestupst? Gestaltungsorientierte Entwicklung von Privacy Nudges vor dem Hintergrund ethischer und rechtlicher Leitlinien. In: Forum Privatheit.

2019

- Barev, T.J.; Janson, A. (2019): Towards an Integrative Understanding of Privacy Nudging – Systematic Review and Research Agenda. Annual Pre-ICIS Workshop on HCI Research. In MIS (Pre-ICIS).
- Schomberg, S.; Barev, T. J.; Janson, A.; Hupfeld, F. (2019): Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging. Datenschutz und Datensicherheit 2019 (43), S. 774-780.
- Schomberg, S.; Barev, T. J.; Janson, A.; Hupfeld, F. (2019): Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging. Informatik 2019 - 49. Jahrestagung der Gesellschaft für Informatik (GI). Gesellschaft für Informatik (GI), Kassel, Germany.

2018

- Janson, A.; Schöbel, S. (2018): Nudging Privacy in Digital Work Systems – Towards the Development of a Design Theory. International Conference on Information Systems (ICIS).

