Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging

Entwicklung erster Szenarien

Sabrina Schomberg[1], Torben Jan Barev[2], Andreas Janson[3] und Felix Hupfeld[4]

Abstract: Die noch recht neue DSGVO hat einige Änderungen mit sich gebracht, welche sich in der Praxis erst noch bewähren und innovativ umgesetzt werden müssen. Insbesondere das Arbeitsumfeld wird von der fortschreitenden Digitalisierung stark verändert und sieht sich neuen Herausforderungen des Datenschutzes gegenüber. Ein Ansatz, diesen Herausforderungen zu begegnen, könnte die Integration von Privacy Nudges in digitale betriebliche Systeme sein. Ziel von Privacy Nudges ist es dabei, den Entscheidungsprozess in digitalen Entscheidungsumgebungen gezielt zu mehr Schutz von personenbezogenen Daten und Privatheit zu beeinflussen. Diesem Ansatz nähert sich dieser Beitrag interdisziplinär, durch Erkenntnisse aus der verhaltensökonomischen, informatischen und der rechtswissenschaftlichen Literatur. Schließlich werden verschiedene Szenarien für den Einsatz von Privacy Nudges in digitalen Arbeitssystemen beschrieben und bewertet.

Keywords: Privacy Nudges, Digital Nudging, Datenschutz durch Technik, Datenschutz „by Design“ und „by Default“, DSGVO

1 Einleitung

Die fortschreitende Digitalisierung und Vernetzung verändert unser Arbeitsumfeld und die Art und Weise, wie wir arbeiten. Mit dieser Entwicklung gehen einerseits erhebliche Innovationspotentiale einher. So können signifikante Synergieeffekte entstehen, aber auch flexiblere und effizientere Arbeitsmodelle. Andererseits birgt die Digitalisierung von Arbeitsprozessen jedoch auch Risiken. Nicht nur für sensible Unternehmensdaten, sondern auch für die Privatheit von Mitarbeiterinnen und Mitarbeitern. In der Regel werden große Datenmengen anfallen, welche leicht ausgewertet werden können, so dass die Gefahr eines gläsernen Arbeitnehmers erwächst. Viele Arbeitnehmerinnen und Arbeitnehmer sind für das Thema Datenschutz auch noch nicht hinreichend sensibilisiert und geben unter Umständen unfreiwillig viele Daten preis. Hinzu kommt noch das sog. Privacy Paradox z.B. [KM16], also die Feststellung, dass Nutzerinnen und Nutzer den

[1] Universität Kassel, FG Öffentliches Recht, IT-Recht und Umweltrecht von Prof. Dr. Hornung, Henschelstraße 4 (K33), 34127 Kassel, sabrina.schomberg@uni-kassel.de.
[2 3 4] Universität Kassel, FG Wirtschaftsinformatik von Prof. Dr. Leimeister, Pfannkuchstraße 1 (ITeG), 34121 Kassel, torben.barev@uni-kassel.de; andreas.janson@uni-kassel.de; felix.hupfeld@wi-kassel.de.

doi:10.18420/inf2019_52

Datenschutz abstrakt wertschätzen und sich um ihre Privatheit sorgen, aber dennoch sorglos mit ihren personenbezogenen Daten umgehen.

Daher sind neue Ansätze gefragt, die die Vorteile der Digitalisierung nutzen, zugleich jedoch auch den Datenschutz nach der DSGVO und nationalen Gesetzen vollumfänglich umsetzen. Hier bieten sich sog. Nudging-Konzepte an, um die Umsetzung zu begleiten [JS18]. Das Nudging („Anstupsen“), welches seinen Ursprung in der Verhaltensökonomik hat [TS08], soll das Verhalten von Nutzerinnen und Nutzern in digitalen Umgebungen vorhersehbar dahingehend beeinflussen, dass sie datenschutzfreundlichere Entscheidungen treffen. Dies geschieht jedoch nicht durch verbindliche Anweisungen oder gar Verbote, sondern durch Aufmerksamkeitslenkungen, spielbasierte Motivationen [SJ18], Voreinstellungen oder andere „weiche“ Instrumente, die Anreize zu einem bestimmten Verhalten geben.

Die Datenschutz-Grundverordnung hat einige Änderungen mit sich gebracht, die sich in der Praxis erst noch bewähren müssen. So ist zum Beispiel erstmals der Datenschutz durch Technik (insb. in Art. 25 DSGVO) normiert. Datenschutz durch Technik bedeutet, dass der Datenschutz schon in die Technik „eingebaut“ ist [La19b]. Diese datenschutzfreundliche Technik soll es gar nicht erst ermöglichen, dass mehr als nur die erforderlichen Daten erhoben, verarbeitet oder gespeichert werden [Ba17]. Dieser Ansatz wurde bereits in den 90iger Jahren diskutiert, bisher jedoch nicht explizit festgeschrieben [BG17]. In Deutschland wurde der Datenschutz durch Technik in den § 3a BDSG a.F., das Prinzip der Datenvermeidung und Datensparsamkeit, hineingelesen. Danach waren auch bisher schon Maßnahmen, insbesondere der Anonymisierung und Pseudonymisierung, zu treffen. Da § 3a BDSG a.F. jedoch nicht bußgeldbewährt war, wurde dieser in der Praxis eher stiefmütterlich behandelt [BG17], [La19b].

Art. 25 DSGVO ist gem. Art. 83 Abs. 4 lit. a DSGVO mit hohen Bußgeldern bedroht. Unternehmen haben daher ein großes wirtschaftliches Interesse daran, den Datenschutz durch Technik nach der DSGVO auch wirklich umzusetzen. Da die Norm jedoch wenig konkrete Maßnahmen benennt, bleibt den Verantwortlichen ein weiter Spielraum bei der Umsetzung [La19b]. Das kann Fluch und Segen zugleich sein. Einerseits sind Unternehmen dadurch nicht an starre Vorgaben gebunden und können einen individuellen Weg der Umsetzung finden. Andererseits besteht eine große Unsicherheit darüber, ob auch die Aufsichtsbehörden diese individuellen Maßnahmen als ausreichend erachten werden.

Ziel dieses Beitrags ist es, im Rahmen eines interdisziplinären Ansatzes, an der Schnittstelle von Recht und Informatik, die Umsetzung der neuen Vorgaben des Datenschutzes durch Technik in der DSGVO durch digitales Nudging im Arbeitsumfeld zu beschreiben und anhand ausgewählter Szenarien zu bewerten.

2 Privacy Nudging im digitalen Kontext

2.1 Grundlagen des Nudgings im digitalen Kontext

Der Begriff *Nudge* beschreibt per Definition eine Methode, um „das Verhalten von Menschen zu beeinflussen, ohne dabei auf Verbote und Gebote zurückgreifen oder ökonomische Anreize verändern zu müssen" [TS08]. Nudging im offline Bereich kann demnach eine Vielzahl von Ansätzen beinhalten, um Entscheidungen zu beeinflussen. Was gewählt wird, hängt oft davon ab, wie die Entscheidungen präsentiert werden [WSV16]. Individuen tendieren beispielsweise dazu, voreingestellte Optionen eher anzunehmen als diese zu verändern [ZX16]. Eines der prominentesten Beispiele für die Effektivität von Nudges stellt hierbei die Organspende in Österreich dar, welche zu einer signifikant höheren Anzahl von Organspendern, beispielsweise im Vergleich zu Deutschland, führt. Entscheidend ist, dass in Österreich die Zustimmung zur Organspende vorausgesetzt wird. Nicht-Spender müssen sich demnach bewusst mit der Entscheidung auseinandersetzen und widersprechen. In Deutschland wird die Zustimmung nicht vorausgesetzt und muss, beispielsweise in einem Organspendeausweis, pro-aktiv festhalten werden [JG03]. Die Entscheidung wird demnach durch eine andere Voreinstellung, oder einen sogenannten Nudge, maßgeblich beeinflusst.

Nudging basiert auf dem Prinzip des libertären Paternalismus, um Entscheidungen zu beeinflussen. Dies bedeutet, dass ein Individuum zu jeder Zeit eine Entscheidungsoption frei wählen kann (Liberalismus-Komponente). In seiner Entscheidungsfreiheit ist das Individuum nicht eingeschränkt, da keine der Optionen verboten und auch der wirtschaftliche Anreiz der Alternativen nicht bemerkenswert verändert wird. Das Individuum wird aber zu der Entscheidungsoption genudged, die für dieses den vermeintlich größten Nutzen darstellt (Paternalismus-Komponente) [MLJ18].

Beim *digitalen Nudging* wird dieses Konzept auf den digitalen Raum übertragen und entsprechende Designelemente in der Benutzeroberfläche verwendet, um das Verhalten in digitalen Entscheidungsumgebungen zu steuern. Digitale Entscheidungsumgebungen sind Benutzeroberflächen, die es erfordern, dass Menschen Urteile oder Entscheidungen treffen [SWV18], beispielsweise für welche Kollegen die eigenen Kalendereinträge einsehbar sein sollen. Besonders gefährlich am digitalen Nuding ist dabei die Möglichkeit der Verknüpfung verschiedener Daten, welche leicht zur Überwachung führen kann, und die bessere Möglichkeit der Personalisierung von Nudges, welche subtile und effektive Manipulation ermöglichen kann [Sa17].

Eine Unterform der digitalen Nudges sind hierbei die sogenannten *Privacy Nudges*. Privacy Nudging beschreibt eine gezielte Beeinflussung des Entscheidungsprozesses, um Menschen dazu zu bringen, dass diese „bessere“ Entscheidungen in Bezug auf deren Privatheit treffen und gleichzeitig ihre informationelle Selbstbestimmung berücksichtigen [Ac17]. Dies birgt jedoch durchaus auch die Gefahr, das Gegenteil zu bewirken und die Privatsphäre der Nutzer zu verletzen. Einerseits, weil es einfacher ist, effektive per-

sonalisierte Nudges zu gestalten, wenn viele persönliche Daten und Verhaltensmuster bekannt sind. Andererseits, weil sich manche Menschen vielleicht auch bewusst dazu entscheiden so viel wie möglich über sich selbst preiszugeben [SK18].

2.2 Grundlegende Prinzipien des Privacy Nudgings

Untersuchungen haben gezeigt, dass insbesondere Nutzer digitaler Systeme aufgrund kognitiver, emotionaler und sozialer Faktoren oft irrational handeln [Ac17], [TSB10]. Dies lässt sich durch die von *Kahnemann* bekannt gewordene Dualprozesstheorie erklären, die besagt, dass Individuen zwei Denksysteme verwenden. Zwei Systeme sind demnach notwendig, um in der heutigen (digitalen) Arbeitswelt den Überfluss an Informationen besser auswerten zu können und gezielt Entscheidungen zu fällen. System 1 stellt hierbei unsere Intuitionen oder unseren unbewussten Autopiloten dar. System 2 hingegen äußert sich durch unser bewusstes Planen und Kontrollieren. Dies erfordert jedoch deutlich mehr mentale Anstrengung und Zeit. Beide Systeme sind gleichzeitig aktiv und arbeiten meist reibungslos zusammen [Ka13], [Ka03]. Im Arbeitsalltag haben die Individuen hingegen selten genügend Zeit und Informationen, um alle Alternativen vollständig zu bewerten. Anstatt einen systematischen Entscheidungsprozess auszuüben, neigen Individuen dazu, auf so genannte Heuristiken (mentale Abkürzungen) zurückzugreifen [HG17]. Heuristiken sind informelle Faustregeln, die die Komplexität der Urteilsfindung reduzieren und somit Abkürzungen in der Entscheidungsfindung darstellen. Heuristiken sind zwar ein effizienter Weg, um wiederkehrende Aufgaben zu lösen, können aber zu systematischen Fehlern wie Verzerrungen in der Informationsbewertung (Biases) führen [Ka13]. So werden beispielsweise personenbezogene Daten oftmals sorglos offengelegt, da das Risiko der unerwünschten Überwachung mental weniger präsent ist (Verfügbarkeitsheuristik). Diese Fehlschlüsse bedeuten nicht, dass das Verhalten von Individuen unberechenbar und irrational ist. Es ist vielmehr eine systematische und vorhersehbare Abweichung vom rationalen Verhalten. An diesem Punkt kommen Privacy Nudges ins Spiel. Privacy Nudges können beide Denksysteme beeinflussen, indem sie Heuristiken ausnutzen oder ihnen entgegenwirken, um Individuen zu ihrer informationellen Selbstbestimmung zu leiten [WSV16].

3 Rechtliche Rahmenbedingung

Im Kontext des Datenschutzes durch digitales Nudging im Arbeitsumfeld ist insbesondere der Datenschutz durch Technik und der Beschäftigtendatenschutz zu beachten. Darüber hinaus müssen natürlich immer auch die allgemeinen Anforderungen der DSGVO eingehalten werden; insbesondere die in Art. 5 DSGVO erstmals kodifizierten Datenschutzgrundsätze. Diese Datenschutzgrundsätze enthalten jedoch eine Reihe unbestimmter Rechtsbegriffe und legen daher lediglich allgemeine Leitlinien fest, welche dann in den weiteren Normen der DSGVO konkretisiert werden [La19a].

3.1 Datenschutz durch Technik

Mit dem Datenschutz durch Technik muss sich der Verantwortliche möglichst früh auseinandersetzen. Bereits im Entwicklungsstadium sollten einige technische Anforderungen beachtet werden, um die personenbezogenen Daten und die Privatsphäre der Nutzerinnen und Nutzer angemessen zu schützen [Ha18].

Alle Maßnahmen der datenschutzfreundlichen Technikgestaltung gem. Art. 25 Abs. 1 DSGVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen auszuwählen und zu treffen. Dies ist Ausdruck des risikobasierten Ansatzes der DSGVO und begrenzt die Auswahl geeigneter technischer Maßnahmen [BH17]. Es bedarf also nicht immer der theoretisch optimalen Maßnahme, sondern bei geringem Risiko oder besonders hohen Implementierungskosten kann im Einzelfall ggf. auch ein geringerer Schutz ausreichend sein. Daher ist eine Verhältnismäßigkeitsabwägung vorzunehmen, welche im Sinne einer allgemeinen Risiko- und Folgenabschätzung dokumentiert werden sollte, um der Rechenschaftspflicht des Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO Genüge zu tun [La19b].

Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO werden wiederum von Teilen der Literatur als eine Konkretisierung der datenschutzfreundlichen Technikgestaltung gem. Art. 25 Abs. 1 DSGVO verstanden, so z.B. [BH17]. Verarbeitungssysteme müssen danach so eingestellt sein, dass nur die für den Zweck der Verarbeitung erforderlichen Daten verarbeitet werden. Es reicht dabei nicht aus, dass der Nutzer eine Wahl- oder Gestaltungsmöglichkeit hat. Personenbezogene Daten dürfen nicht ohne Kenntnis und ohne Zustimmung des Betroffenen verarbeitet werden [Ri18]. Die Zulässigkeit einer Systemeinstellung beurteilt sich also danach, ob die Verarbeitung hinsichtlich Menge, Umfang, Speicherfrist und Zugänglichkeit der personenbezogenen Daten für den Zweck erforderlich ist [Ri18].

Martini war der erste Autor, der im Kontext des Art. 25 Abs. 2 DSGVO das Wort „Nudging“ verwendete [Ma17]. Er geht allerdings von „Nudging mit umgekehrter Stoßrichtung“ durch die DSGVO aus, da die Dienstanbieter nun ihre eigenen wirtschaftlichen Interessen dem Gebot der Datenminimierung unterordnen müssen [Ma18]. *Thaler* und *Sunstein* können aber viel eher so verstanden werden, dass Art. 25 Abs. 2 DSGVO genau die Intention der Autoren von „Nudge“ trifft. Denn es geht um „bessere“ Entscheidungen für den Nutzer und nicht für den Dienstanbieter; also den Angestupsten und nicht den Entscheidungsarchitekten [TS08]. Dass die Dienstanbieter Voreinstellungen datenschutzfreundlich und nicht maximal vorteilhaft für die eigene Gewinnerzielung ausgestalten, wäre daher mutmaßlich auch im Sinne von *Thaler* und *Sunstein*.

Privacy Nudges in Form von datenschutzfreundlichen Voreinstellungen sind mithin in Art. 25 Abs. 2 DSGVO ausdrücklich vorgesehen [HB17]. Fraglich ist, ob darunter auch weitere digitale Nudges gefasst werden können. Bei Auslegung des Wortlauts von Art. 25 Abs. 2 DSGVO dürfte es schwer sein neben Default Nudges, also Voreinstellungen,

auch weitere Arten von Nudges unter diesen zu subsumieren. Weitere Nudges könnten als technische und organisatorische Maßnahmen jedoch unter Art. 25 Abs. 1 DSGVO zu fassen sein. Der Wortlaut des Abs. 1 ist weiter und so unkonkret, dass er durch die Verantwortlichen ausgestaltet werden muss. Eine mögliche Ausgestaltung könnte die Verwendung datenschutzfreundlicher Nudges sein. Dies passt auch insoweit in die Systematik, als dass Art. 25 Abs. 2 DSGVO eine Konkretisierung des Absatz 1 ist (s.o.). Desweitern dürfte dies im Sinne des Verordnungsgebers sein, sofern so personenbezogene Daten geschützt werden können, ohne die Betroffenen ihrer Entscheidungsfreiheit zu berauben (vgl. Art. 1 Abs. 2 DSGVO).

Nach Art. 25 Abs. 3 DSGVO kann eine erfolgreiche Zertifizierung im Sinne des Art. 42 DSGVO oder die Einhaltung genehmigter Verfahrensregeln (Art. 40 Abs. 2 lit. h DSGVO) als ein Faktor herangezogen werden, um die Erfüllung der Anforderungen der Norm nachzuweisen [La19b].

Adressat des Art. 25 DSGVO ist ausdrücklich nur der Verantwortliche, nicht jedoch der Hersteller von Verarbeitungstechnik. Für den Hersteller besteht daher grundsätzlich keine Pflicht zur datenschutzfreundlichen Ausgestaltung seiner Produkte. Er wird lediglich durch Erwägungsgrund 78 dazu „ermutigt“ [BH17]. Da für die Verantwortlichen jedoch eine hohe Strafe droht, werden sie nur solche Produkte kaufen, die den Anforderungen der DSGVO gerecht werden. Deshalb besteht indirekt doch eine Verpflichtung der Hersteller, die typischerweise durch entsprechende Vertragsklauseln umgesetzt werden wird [Ha18].

Der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gem. Art. 25 DSGVO wird als Konkretisierung der Pflicht zur Umsetzung technischer und organisatorischer Maßnahmen durch den Verantwortlichen gem. Art. 24 DSGVO verstanden [Ma18]. Art. 25, Art. 32 und Art. 35 DSGVO sind so eng verzahnt, dass sich eine gemeinsame Bearbeitung der verschiedenen Schritte und Prüfungen anbietet. Art. 25 und Art. 32 DSGVO ähneln sich schon vom Wortlaut so sehr, dass eine klare Differenzierung zwischen Maßnahmen gem. Art. 25 DSGVO und Maßnahmen nach Art. 32 DSGVO kaum möglich sein wird. Ohne die Folgenabschätzung gem. Art. 35 DSGVO wiederum wird es kaum möglich sein, die Risiken, die mit der Datenverarbeitung einhergehen, abzuschätzen und dementsprechende Maßnahmen zu ergreifen [Ha18].

3.2 Beschäftigtendatenschutz

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 [KM16]. 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 [Wy17], [TR16], [Ko17]. 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.

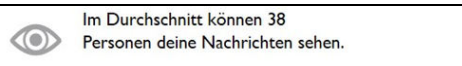
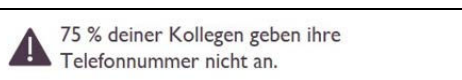
Der deutsche Gesetzgeber hat davon in § 26 BDSG Gebrauch gemacht und orientierte sich dabei erkennbar an § 32 BDSG a.F., welcher zuvor den Beschäftigtendatenschutz regelte [Wy17]. So wurde der Kern der alten Regelung übernommen und es werden nach wie vor alle drei Phasen des Beschäftigungsverhältnisses, nämlich die Begründung, dessen Durchführung und dessen Beendigung, erfasst. Diese strukturelle Ähnlichkeit soll für eine gewisse Kontinuität im deutschen Beschäftigtendatenschutz sorgen [Ko18]. Inhaltlich geht die neue deutsche Regelung des Beschäftigtendatenschutzes jedoch deutlich über die bisherige hinaus [Ko17].

§ 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 Arbeitgebern und Arbeitnehmern Rechnung zu tragen, werden mit Art. 26 Abs. 2 BSDG jedoch erhöhte Anforderungen an die Freiwilligkeit der Einwilligung gestellt. Der Arbeitgeber muss bei der Beurteilung der Freiwilligkeit immer die im Beschäftigungsverhältnis bestehende Abhängigkeit des Beschäftigten berücksichtigen. Von der Freiwilligkeit der Einwilligung ist jedoch auszugehen, wenn für den Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder sofern Arbeitgeber und Beschäftigter gleichgelagerte Interessen verfolgen [Wy17]. Eine Einwilligung der Arbeitnehmer in die Verarbeitung ihrer personenbezogenen Daten mit inkludierten Privacy Nudges dürfte daher auch unproblematisch möglich sein, da in der Regel sowohl der Arbeitgeber als auch der Arbeitnehmer ein Interesse an datenschutzfreundlicher Ausgestaltung der Datenverarbeitung haben. Beschäftigte müssen jedoch über ihr Widerrufsrecht gem. Art. 7 Abs. 3 DSGVO aufgeklärt werden.

Problematischer könnte allerdings die unklare Rolle des Betriebsrats sein. Weder die DSGVO noch § 26 BDSG befassen sich mit der Frage, ob der Betriebsrat eigenständiger Datenverarbeiter oder Teil des Arbeitgebers als der für die Datenverarbeitung Verantwortliche ist [Ko17], [Ko18]. Der Betriebsrat könnte gem. § 87 BetrVG ein Mitbestimmungsrecht bei der Ausgestaltung der 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 Szenarien für den Einsatz von Privacy Nudges in digitalen Arbeitssystemen

Um Szenarien für Privacy Nudges zu entwickeln, wurden in einer systematischen Literaturrecherche sechs Privacy Nudge Prinzipien identifiziert, welche nachfolgend mit ihren speziellen Biases, Heuristiken und Prinzipien näher betrachtet werden. Zusätzlich werden Szenarien, in denen sie eingesetzt werden können, näher erläutert. Dabei beziehen wir uns insbesondere auf die bestehende Typologisierung von Privacy Nudges nach *Acquisti et al.* [Ac17] und erweitern diese Sichtweise entsprechend um den Kontext digitaler Arbeitssysteme im Betrieb. Zur Veranschaulichung führen wir in Tabelle 1 zu jedem Privacy Nudge ein Beispiel auf. Die Vorgehensweise der systematischen Literaturrecherche orientiert sich an der vorgeschlagenen Methodik von *vom Brocke et al.* [Vo15]. Um die Thematik der Privacy Nudges umfassend zu erfassen, wurde auf Beiträge aus sechs verschiedenen Datenbanken zugegriffen. Neben der AIS eLibray wurden die ACM Digital Library und die IEEE Xplore Digital Library als klassische Repräsentanten der Datenbanken im Bereich Informationssysteme ausgewählt. Das Social Science Research Network (SSRN), ScienceDirect und EBSCOhost wurden hinzugenommen, um auch verhaltensbezogene und psychologische Quellen gezielt zu integrieren. Die deutsche Literatur wurden mit englischsprachigen Beiträgen ergänzt, um den internationalen Stand der Forschung abzubilden.

Privacy Nudge	**Beispiel**
Default	
Farbelemente	
Information	
Feedback	
Zeitverzögerung	
Soziale Norm	

Tab.1: Beispiele digitaler Privacy Nudges im Arbeitsumfeld

Defaults

Default Nudges beschreiben Standardeinstellungen im System. Da Individuen in digitalen Umgebungen die Privatsphäre-Einstellungen häufig nicht ihren Bedürfnissen anpassen, bleibt die voreingestellte Option (der Status-quo) übermäßig bevorzugt und meist unverändert (Status-quo Bias) [Ac17], [TS08]. Zudem wird die voreingestellte Option als Referenzpunkt für das Abwägen der Entscheidungsoptionen herangezogen. Dieser „Anker" wird von Individuen unbewusst wahrgenommen. Jede Entscheidungsoption wird nun gegen diese Alternative abgewägt und das Entscheidungsverhalten in diese Richtung beeinflusst [TK74]. *Hummel* und *Maedche* bewerten Defaults tendenziell als die stärksten Nudges [HM19]. In Bezug auf Privacy Nudging gelten Defaults als sehr effektiv, da sie in digitalen Arbeitssystemen standardmäßig das Maß der Datensparsamkeit vorgeben [Ac17].

Farbelemente

Auch Farbelemente können als Privacy Nudges verwendet werden. Farbliche Hinterlegungen lenken hierbei die Aufmerksamkeit auf ausgewählte Elemente, um bestimmte Entscheidungsalternativen verstärkt hervorzuheben. Bei mobilen Apps kann beispielsweise die Schaltfläche zur Datenfreigabe farblich stärker betont werden. Im aufgezeigten Beispiel wird der „privat"-Button in grüner Farbe markiert und Individuen dazu angehalten, diese Option zu wählen. Im Rahmen der digitalen Arbeit wären sensible Daten nun ausschließlich für eine bestimmte Zielgruppe oder nur für das Individuum selbst zugänglich [Al15]. Die Vorteile der Farbelemente zeigen sich vor allem in der einfachen Umsetzung solcher Nudges, die das Individuum schnell und effektiv dazu bewegen, seine Entscheidungen bezüglich des Datenschutzes und der Privatsphäre zu überdenken.

Information

Die Wahrscheinlichkeit einer Verletzung der Privatsphäre ist häufig für Individuen nicht nachvollziehbar und wird oft unterschätzt. Das Individuum tendiert dann dazu, am Arbeitsplatz 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 [Ac17], [TK74]. Um diesen Heuristiken entgegenzuwirken, wird das Individuum über Risiken und Konsequenzen seines Handelns aufgeklärt. Basierend auf diesen Informationen kann das Individuum eine fundierte Entscheidung in Bezug auf die eigene Privatsphäre treffen [Ac17].

Feedback

Einen weiteren Privacy Nudge stellt die Bereitstellung von Feedback dar, welches auf das bisherige Nutzungsverhalten einer Person hinweist. Dies schafft beim Individuum ein Bewusstsein über seine bisherigen und aktuellen Entscheidungen und dessen Konse-

quenzen [Ac17]. Ein Beispiel für Privacy Nudging durch Feedback ist ein Fortschritts-Balken, der z.B. beim Registrierungsprozess im Arbeitssystem die Stärke eines Passworts illustriert oder die Menge der eingegebenen Daten im Profil widerspiegelt. So werden Individuen spielerisch dazu angehalten, ein komplexeres Passwort zu wählen bzw. weniger Daten im System zu hinterlegen.
Entscheidend für ein erfolgreiches Nudging durch Feedback ist die Art und Weise der Darstellung. Insbesondere Textbenachrichtigungen ohne Ton, die den Arbeitsfluss nicht einschränken, gelten als effektiv [Mi17].

Zeitverzögerung

Bei digitalen Entscheidungen über die Privatsphäre werden oftmals risikoreiche und wenig durchdachte Entscheidungen ohne Anbetracht der möglichen Spätfolgen begünstigt. Dem zugrunde liegt das sogenannte Hyperbolic Discounting, bei dem der unmittelbare Nutzen überschätzt und später eintretende Kosten unterschätzt werden [Ac17]. Um diesem entgegenzuwirken, kann eine zeitliche Verzögerung als Privacy Nudge verwendet werden [Wa14]. Beispielsweise wird ein Countdown von fünf Sekunden eingesetzt, bevor eine Nachricht mit riskanten Inhalten im Firmennetzwerk veröffentlicht wird. In diesen Sekunden besteht weiterhin die Möglichkeit, die Nachricht zurückzuziehen, zu bearbeiten oder die Wartezeit direkt zu überspringen. So soll das Individuum dazu bewegt werden, weniger impulsiv zu agieren sowie die Nachricht und mögliche negative Konsequenzen zu überdenken [Ac17]. Während die Zeitverzögerung große Effektivität verspricht, sollte beim Einsatz dieses Privacy Nudges bedacht werden, dass die Verzögerung der Aktion auch als störend empfunden werden kann.

Soziale Norm

Die Wirkung dieses Privacy Nudges basiert auf dem Prinzip der sozialen Normen. Das Individuum leitet dabei aus dem Verhalten seiner Mitmenschen ab, inwiefern es angemessen ist, persönliche Informationen zu teilen [Ch16], [Co16]. Beispielsweise ist für das Individuum erkenntlich, dass 75 % Prozent der Kollegen die eigene Telefonnummer nicht im Arbeitsprofil angegeben haben. Diese Information wird nun als Referenzpunkt für das eigene Verhalten herangezogen (Ankerheuristik) [Ac17]. Eine Studie im Rahmen der Vergabe von Zugriffsberechtigungen für Smartphone Apps hat dabei gezeigt, dass die soziale Norm auch entgegen einer Datensparsamkeit wirken kann. Falls die Mehrheit den Zugriff einer App auf bestimmte Daten zulässt, könnten Individuen dazu verleitet werden, sich ebenso zu verhalten [ZX16]. Diese Nudges sollten daher mit Bedacht verwendet werden, um Individuen zu besseren Entscheidungen in Bezug auf den Schutz ihrer Daten zu befähigen [Ch16].

5 Abschließende Bewertung

Privacy Nudges können eine effektive Methode darstellen, das Verhalten von Nutzerinnen und Nutzern in digitalen Arbeitsumgebungen vorhersehbar dahingehend zu beein-

flussen, dass sie datenschutzfreundlichere Entscheidungen treffen. Die Wirkung der Privacy Nudges ist dabei stark vom Kontext abhängig. Die vorgestellten Szenarien können bei der Auswahl der richtigen Nudges unterstützen, damit diese ihre volle Wirkung entfalten. Außerdem sollten die Nudges so gewählt werden, dass diese den Arbeitsprozess nicht behindern. Insbesondere bei Nudges, welche auf dem Prinzip der sozialen Norm basieren, ist darauf zu achten, dass diese nicht in die falsche Richtung wirken und die Arbeitnehmer zu mehr Datenoffenlegung verleiten. Generell sollten Nudges möglichst transparent gestaltet sein, um der Gefahr der Manipulation entgegenzuwirken.

Die Personalisierung von Nudges kann zudem deren Effektivität zusätzlich erhöhen [Su15]. Dies könnte daher ein vielversprechender, weitergehender Schritt für Privacy Nudges sein. Dafür ist zu erforschen, wie personalisierte Nudges automatisch umgesetzt werden könnten und welche neuen rechtlichen Fragestellungen sich daraus ergeben. Zudem könnten edukative Nudges, welche zur Reflektion über die Preisgabe von Daten anregen, Lernprozesse befördern und damit Nutzer digitaler Angebote befähigen, bessere Entscheidungen hinsichtlich ihrer Privatsphäre zu treffen.

Bei den Default Nudges in digitalen Arbeitssystemen handelt es sich um eine Maßnahme im Sinne des Art. 25 Abs. 2 DSGVO. Die Literatur legt nahe, dass Default Nudges am effektivsten sind, da sie in digitalen Arbeitssystemen standartmäßig das Maß der Datensparsamkeit vorgeben (vgl. Kapitel 4). Alle anderen vorgestellten Beispiele digitaler Privacy Nudges im Arbeitsumfeld wären nach der hier vertretenen Auffassung (siehe 3.1) rechtlich als Datenschutzmaßnahmen durch Technikgestaltung gem. Art. 25 Abs. 1 DSGVO einzuordnen.

Um die Vorgaben des Art. 25 DSGVO vollständig im Unternehmen umzusetzen und sich nicht der Gefahr eines hohen Bußgeldes gem. Art. 83 Abs. 4 DSGVO auszusetzen werden weitere technische und organisatorische Maßnahmen zu treffen sein. Privacy Nudges können jedoch eine dieser Maßnahme im Sinne des Art. 25 DSGVO sein, um den Schutz von personenbezogenen Daten und der Privatheit von Mitarbeiterinnen und Mitarbeitern zu verbessern. Somit können Privacy Nudges einen wichtigen Beitrag dazu leisten den sehr abstrakten Art. 25 DSGVO mit Leben zu füllen.

Danksagung

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

Literaturverzeichnis

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

[Al15] Almuhimedi, H. et al.: Your Location has been Shared 5,398 Times! In (Begole, B. et al. Hrsg.): Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15. ACM Press, New York, New York, USA, 2015; S. 787–796.

[Ba17] Barlag, C.: § 3 VII. Datenschutz durch Technikgestaltung. In (Roßnagel, A. Hrsg.): Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts. Nomos, Baden-Baden, 2017.

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

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

[Ch16] Chang, D. et al.: Engineering Information Disclosure: CHI'16 Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems; S. 587–597.

[Co16] Coventry, L. M. et al.: Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. In Frontiers in psychology, 2016, 7; S. 1341.

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

[HB17] Herfurth, C.; Benner-Tischler, A.: Nudging in der DS-GVO und die Wirkung von Privacy by Default. In ZD-Aktuell, 2017.

[HG17] Hertwig, R.; Grüne-Yanoff, T.: Nudging and Boosting: Steering or Empowering Good Decisions. In Perspectives on psychological science a journal of the Association for Psychological Science, 2017, 12; S. 973–986.

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

[JG03] Johnson, E. J.; Goldstein, D.: Medicine. Do defaults save lives? In Science (New York, N.Y.), 2003, 302; S. 1338–1339.

[JS18] Janson, A.; Schöbel, S.: Nudging Privacy in Digital Work Systems. Towards the Development of a Desgin Theory. In International Conference on Information Systems (ICIS), 2018.

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

[Ka13] Kahneman, D.: Thinking, fast and slow. Farrar, New York, 2013.

[KM16] Kühling, J.; Martini, M.: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Detenschutzrecht? In EuZW, 2016; S. 448–453.

[Ko17] Kort, M.: Der Beschäftigtendatenschutz gem. § 26 BDSG-neu. Ist die Ausfüllung der Öffnungsklausel des Art. 88 DS-GVO geglückt? In ZD, 2017; S. 319–323.

[Ko18] Kort, M.: Die Bedeutung der neueren arbeitsrechtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes. In NZA, 2018; S. 1097–1105.

[La19a] Laue, P.: § 1. Einführung. In (Laue, P.; Kremer, S. Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis. Nomos, Baden-Baden, 2019.

[La19b] Laue, P.: § 7. Technischer und organisatorischer Datenschutz. In (Laue, P.; Kremer, S. Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis. Nomos, Baden-Baden, 2019.

[Ma17] Martini, M.: Art. 25. In (Paal, B. P.; Pauly, D. A. Hrsg.): Datenschutz-Grundverordnung. C.H.Beck, München, 2017.

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

[Mi17] Micallef, N. et al.: Stop annoying me! In (Soro, A. et al. Hrsg.): Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17. ACM Press, New York, New York, USA, 2017; S. 371–375.

[MLJ18] Tobias Mirsch, Christiane Lehrer, and Reinhard Jung: Making Digital Nudging Applicable: The Digital Nudge Design Method: Thirty Ninth International Conference on Information Systems, San Francisco.

[Ri18] Richter, P.: Datenschutz durch Technik und datenschutzfreundliche Voreinstellung. In (Jandt, S.; Steidle, R. Hrsg.): Datenschutz im Internet. Rechtshandbuch zu DSGVO und BDSG. Nomos, Baden-Baden, 2018; S. 356–374.

[Sa17] Sascha Lobo: Nudging - Du willst es doch auch. Oder? In Spiegel Online, 2017.

[SJ18] Schöbel, S.; Janson, A.: Is it All About Having Fun? - Developing a Taxonomy to Gamifiy Information Systems. In ECIS 2018 Proceedings, 2018.

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

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

[SWV18] Schneider, C.; Weinmann, M.; Vom Brocke, J.: Digital nudging. In Communications of the ACM, 2018, 61; S. 67–73.

[TK74] Tversky, A.; Kahneman, D.: Judgment under Uncertainty: Heuristics and Biases. In Science (New York, N.Y.), 1974, 185; S. 1124–1131.

[TR16] Taeger, J.; Rose, E.: Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes. In BB (Betriebs-Berater), 2016; S. 819–831.

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

[TSB10] Thaler, R. H.; Sunstein, C. R.; Balz, J. P.: Choice Architecture. In SSRN Electronic Journal, 2010.

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

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

[Wy17] Wybitul, T.: Der neue Beschäftigtendatenschutz nach Art. 26 BDSG und Art. 88 DSGVO. In NZA, 2017; S. 413–419.

[ZX16] Zhang, B.; Xu, H.: Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In (Gergle, D. et al. Hrsg.): Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16. ACM Press, New York, New York, USA, 2016; S. 1674–1688.