M. Vorschläge zur Anpassung der DSGVO

Laut einer Umfrage geben 74 % der Verantwortlichen an, dass Rechtsunsicherheit die größte Herausforderung bei der Umsetzung der DSGVO ist. Diese Unsicherheit kann entweder kleinschrittig durch konkretisierende Rechtsprechungen oder allgemein durch eindeutigere Gesetze und Infomaterialien beseitigt werden. Letzteres ist die effektivere Option, da damit schlagartig Gewissheit hergestellt werden kann. Bei Gesetzesanpassungen sind allerdings drei Aspekte zu berücksichtigen:

1. Die Anpassungen müssen nachhaltig sein, also in einer Art und Weise formuliert werden, dass eine zeitlich konstante Gültigkeit auch mit veränderten Bedingungen gegeben ist,
2. Gesetzesanpassungen müssen genug Klarheit bieten, ohne die individuelle Freiheit der Verantwortlichen, auch eigenständig innovative Lösungen für konkrete Probleme zu finden, einzuschränken und
3. Die Anpassung sollte den derzeitigen Stand der Wissenschaft berücksichtigen, aber möglichen zukünftigen Erkenntnisgewinn nicht ausschließen.

Gesetzgebung und -anpassung sind demnach eine enorme Herausforderung. Nichtsdestotrotz soll hier der Versuch gewagt werden, eine ergebnisorientierte Anpassung der DSGVO zu erarbeiten, die die identifizierten Schwachstellen in Bezug auf die zukünftige Regulierung von BCI und der damit einhergehenden Verarbeitung von Wesensdaten ausbessern soll.

I. Anwendungsbereich: Möglicher zukünftiger Umgang mit besonderen Kategorien von personenbezogenen Daten

Wie ausgeführt wurde, ist in vielen Fällen nicht klar, wie die Bestimmung von besonderen Kategorien von personenbezogenen Daten vorgenommen werden muss. Besonders in Bezug auf Wesensdaten kann sich dies für Betroffene nachteilig auswirken. Um dieses Problem aufzulösen, sollte ein verbesserter Umgang mit sensitiven Daten gefunden werden.

1. Einfache Maßnahmen

a. Vorgaben von Aufsichtsbehörden

Denkbar wäre bspw. eine analoge Herangehensweise zu Art. 35 Abs. 5 DSGVO, bei der Aufsichtsbehörden Listen herausgeben, für Arten von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung notwendig ist. In Bezug auf besondere Kategorien von personenbezogenen Daten könnte eine ähnliche Klausel im Reglungsbereich des Art. 9 DSGVO einige Ungewissheiten beseitigen. Aufsichtsbehörden könnten somit definieren, welche Verarbeitungszwecke und welche Verarbeitungskontexte in der Regel dafürsprechen, dass sensitive Informationen vorliegen und die Ergebnisse allgemein zugänglich machen. Diese Liste sollte allerdings nicht abschließend sein, jedoch als Ziel haben, die wichtigsten Fälle abzudecken.

Dieses Vorgehen würde auf Seiten der Verantwortlichen für mehr Handlungssicherheit und auf Seiten der Betroffenen für mehr Transparenz sorgen. Ebenso wäre daran vorteilhaft, dass die Liste kontinuierlich erweitert und angepasst werden kann. Auf neue Urteile oder neue Technologien wie bspw. BCI könnte ohne Probleme seitens der Aufsichtsbehörde reagiert werden, indem entsprechende Verarbeitungszwecke und Verarbeitungskontexte auf der Liste ergänzt werden würden.

Nachteilhaft ist daran allerdings, dass Aufsichtsbehörden mit diesem Vorgehen mit einem hohen initialen Aufwand (erstmaliges Ausarbeiten der Liste) konfrontiert werden. Ebenso sind die Pflege und Aktualisierung der Liste mit konstantem weiterem Aufwand verbunden. Die Tatsache, dass in Art. 35 Abs. 3 lit. c DSGVO bezüglich Datenschutz-Folgenabschätzungen bereits erwähnt wird, dass für die umfangreiche Verarbeitung von besonderen Kategorien von personenbezogenen Daten eben jenes besondere Risk-Assessment notwendig ist, lässt allerdings darauf schließen, dass in den ggf. schon bestehenden Listen der Aufsichtsbehörden gemäß Art. 35 Abs. 5 DSGVO bereits etliche Verarbeitungstätigkeiten enthalten sein dürften, die ebenso für den Fall der Bestimmung von besonderen Kategorien von personenbezogenen Daten herangezogen werden könnten. Dies würde den Aufwand für die Aufsichtsbehörden entsprechend vermindern.

b. Anpassung der Informationspflicht

Die Informationspflicht nach Art. 13 u. 14 DSGVO ist ein zentrales Element, um die informationelle Selbstbestimmung der betroffenen Personen

zu ermöglichen. Durch die Bereitstellung der Informationen soll ein Verständnis für den Umfang und die Auswirkung der Datenverarbeitung vermittelt werden. Dies befähigt Betroffene bspw. dazu, ihre speziellen Rechte aus Art. 15 – 23 DSGVO wahrzunehmen.

Art. 13 u. 14 Abs. 1 u. 2 DSGVO geben vor, welche genauen Informationen der Verantwortliche bereitstellen muss. So müssen bspw. die Kontaktdaten des Verantwortlichen, der Zweck und die Rechtsgrundlage der Verarbeitung, die Speicherdauer und die Übermittlung der Daten an mögliche Dritte transparent gemacht werden. Die Kategorie der betroffenen Daten ist nur unter dem Reglungsbereich von Art. 14 Abs. 1 lit. d DSGVO mitzuteilen. Das bedeutet, dass nur dann darüber aufgeklärt wird, welche Daten verarbeitet werden, wenn die Daten nicht bei der betroffenen Person selbst erhoben werden. Diese Unterscheidung erscheint nicht überzeugend. Auch wenn Daten direkt bei der betroffenen Person erhoben werden, muss das nicht immer heißen, dass die Kategorien von betroffenen Daten offensichtlich sind. Wenn eine Person bspw. ein Kontaktformular auf einer Webseite nutzt, füllt diese zwar die Pflichtfelder aus und weiß somit, welche offensichtlichen Daten verarbeitet werden, unbekannt ist ihr aber, dass z.B. auch ihre IP-Adresse o.Ä. mit übermittelt wird. Diese Tatsache sollte vom Verantwortlichen transparent gemacht werden, auch wenn eine direkte Erhebung bei der betroffenen Person stattfindet.

Es ist zudem weder in Art. 13 DSGVO noch in Art. 14 DSGVO vorgesehen, dass die betroffene Person explizit über die Verarbeitung besonderer Kategorien personenbezogener Daten informiert werden muss. Zwar fallen besondere Kategorien von personenbezogenen Daten auch unter Art. 14 Abs. 1 lit. d DSGVO, allerdings ist es nicht gefordert, diese auch entsprechend als solche zu kennzeichnen. Für Betroffene wäre dies hilfreich, da der Status als besondere Kategorie von personenbezogenen Daten oftmals schwer erkenntlich ist. Nutzt eine Person bspw. eine App, mit der die Ernährung getrackt und analysiert wird, um Krankheitsgefährdungspotentiale frühzeitig zu erkennen, ist es nicht unbedingt direkt ersichtlich, dass eine Verarbeitung von Gesundheitsdaten vorliegt. Dieses Wissen ist für Betroffene aber essenziell, um bewerten zu können, ob sie bspw. in diese Verarbeitung einwilligen. Verantwortliche sollten also explizit angeben müssen, wenn die betroffenen Daten in den Reglungsbereich von Art. 9 Abs. 1 DSGVO fallen und auch darlegen, wieso dies der Fall ist.

Besonders bei der zukünftigen Verarbeitung von Wesensdaten wird dies relevant werden. Wie bereits dargelegt, ist die Einstufung von Wesensdaten als besondere Kategorien von personenbezogenen Daten besonders

schwierig. Demnach wird diese Einordnung auch für betroffene Personen herausfordernd sein. Allerdings sollten diese vor der Verarbeitung eindeutig darauf hingewiesen werden, dass hoch sensitive Wesensdaten von ihnen verarbeitet werden und warum diese Daten als besondere Kategorien von personenbezogenen Daten einzustufen sind.

2. Ein neues System: Die Abschaffung von besonderen Kategorien von personenbezogenen Daten

Eine andere Lösung für das Problem mit der Bestimmung von sensitiven Daten erfordert ein fundamentales Umdenken im Datenschutzrecht. Betrachtet man die wachsende Rechenkraft, den zunehmenden Einsatz von Big Data und auch die Entwicklung im Bereich der künstlichen Intelligenz, kann zu dem Schluss gekommen werden, dass letztendlich alle Datenarten das Potential in sich tragen, hoch sensible Aussagen über die betroffene Person zu machen.[798] Beispielhaft dafür ist das Auswertungspotential von Likes oder Kommentaren auf Social Media, wodurch bspw. politische Einstellungen zuverlässig vorhergesagt werden können.[799] Gemäß diesen Gegebenheiten und der entsprechenden technologischen Entwicklung, stellt sich die grundsätzliche Frage, ob eine Unterscheidung zwischen personenbezogenen Daten und besonderen Kategorien von personenbezogenen Daten überhaupt noch zeitgemäß ist.[800]

Die Beseitigung der zweigleisigen Regulierung von personenbezogenen Daten würde dazu führen, dass die schwierige Einstufung des Vorliegens von besonderen Kategorien von personenbezogenen Daten entfallen würde. Dies dürfte aber nicht dazu führen, dass ein insg. geringer Schutz für die ehemals besonderen Kategorien von personenbezogenen Daten entsteht. Sollte eine Aufhebung der Unterscheidung stattfinden, muss vielmehr

798 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1596 f. und 1599); *Frenzel* (2021), Art. 9 Rn. 8*; Moerel/Prins:* Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things, v. 25.5.2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 (abgerufen 5.1.2025).

799 *Chester/Montgomery,* Internet Policy Review 2017, S. 1 (7); *Zuiderveen Borgesius et al.,* Utrecht Law Review 2018, S. 82 (82); *Christl,* Aus Politik und Zeitgeschichte 2019, S. 42 (46 ff.).

800 *Moerel/Prins:* Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things, v. 25.5.2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 (abgerufen 5.1.2025).

sichergestellt werden, dass die betroffene Person und ihre informationelle Selbstbestimmung weiterhin so gut wie möglich geschützt werden. Mit dieser Prämisse als Grundlage, soll nun versucht werden, ein ganz neues System zu entwerfen.

Der bisher größte Unterschied zwischen personenbezogenen Daten und besonderen Kategorien von personenbezogenen Daten ist die gesetzliche Legitimierung, die eine Verarbeitung der jeweiligen Daten rechtfertigt. Im Vergleich zu Art. 6 Abs. 1 DSGVO sieht Art. 9 Abs. 2 DSGVO z.B. keine Möglichkeit vor, dass besondere Kategorien von personenbezogenen Daten auf Grundlage eines Vertrags oder zur Vertragsanbahnung sowie aufgrund eines berechtigten Interesses des Verantwortlichen oder eines Dritten verarbeitet werden können.

Die nachfolgende tabellarische Übersicht soll weitere Unterschiede bzgl. der Rechtsgrundlagen darstellen. Ebenso sollen damit Möglichkeiten aufgezeigt werden, wie diese unterschiedlichen Vorgaben sinnvollerweise zu einem einheitlichen Regulierungsregime zusammengeführt werden könnten.

Art. 6 Abs. 1 DSGVO	**Art. 9 Abs. 2 DSGVO**	**Neues einheitliches System**
Einwilligung (lit. a)	Ausdrückliche Einwilligung (lit. a)	Ausdrückliche Einwilligung
Vertrag (lit. b)	-	Vertrag, solange dadurch keine wesentlichen Beeinträchtigungen der informationellen Selbstbestimmung der betroffenen Person ermöglicht werden (genauere Ausführung in Kapitel M.I.2.b)
Rechtliche Verpflichtung (lit. c)	Einhaltung und Ausübung von Arbeitsrecht, Recht der sozialen Sicherheit und des Sozialschutzes (lit. b) und die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich (lit. f)	Rechtliche Verpflichtung und Einhaltung und Ausübung von Arbeitsrecht, Recht der sozialen Sicherheit und des Sozialschutzes sowie Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit

Art. 6 Abs. 1 DSGVO	Art. 9 Abs. 2 DSGVO	Neues einheitliches System
Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person (lit. d)	Ergänzung: Solange die betroffene Person außerstande ist, ihre Einwilligung zu geben (lit. c)	Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person, solange die betroffene Person außerstande ist, ihre Einwilligung zu geben
Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen (lit. e)	Erhebliches öffentliches Interesse, bei dem Grundrechte, Interessen und Datenschutz gewahrt werden müssen und öffentliches Interesse bzgl. Archivzwecke und öffentlicher Gesundheit, bei dem Angemessenheit, Grundrechte, Interessen und Datenschutz gewahrt werden müssen (lit. g, i, j)	Wahrnehmung von Aufgaben, die im ausreichenden öffentlichen Interesse liegen, bei dem Angemessenheit, Grundrechte, Interessen und Datenschutz gewahrt werden müssen (genauere Ausführung in Kapitel M.I.2.a)
Berechtigtes Interesse (lit. f)	-	Berechtigtes Interesse mit ergänzenden Sicherheitsmechanismen (genauere Ausführung in Kapitel M.I.2.c)
-	Geeignete Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten (lit. d)	Geeignete Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten (lit. d)
-	Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat (lit. e)	Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat (lit. e)
	Gesundheitsvorsorge, Arbeitsmedizin etc. (lit. h)	Gesundheitsvorsorge, Arbeitsmedizin etc. (lit. h)

Die Gegenüberstellung zeigt, dass eine sinnvolle Zusammenführung der beiden Reglungsbereiche möglich ist.

b. Einfache Anpassungen

Die Einwilligung würde im neuen System zu einer ausdrücklichen Einwilligung umformuliert werden. Wie bereits in Kapitel aufgezeigt G.II.2 wurde, ist es grundsätzlich und unabhängig der betroffenen personenbezogenen Daten sinnvoll, hohe Anforderungen an die Einwilligung zu stellen. Dies würde mit der allgemeinen Anforderung nach einer ausdrücklichen Einwilligung Rechnung getragen werden. Die Einwilligung muss sich demnach ausdrücklich auf die Verarbeitung beziehen. Eine konkludente Einwilligung soll damit komplett ausgeschlossen werden.[801] Dies erfordert, dass die betroffene Person genaustens über die geplante Verarbeitung inkl. der besonderen Kategorien von personenbezogenen Daten informiert wird, da nur so eine eindeutige und zweifelsfreie Einwilligung zustande kommen kann.[802] Entsprechend gelten hohe Ansprüche bzgl. Genauigkeit und Transparenz.[803]

Die rechtliche Verpflichtung gemäß Art. 6 Abs. 1 lit. c DSGVO würde mit den Vorgaben des Art. 9 Abs. 2 lit. b u. f DSGVO zusammengeführt werden. Die lebenswichtigen Interessen, die nach Art. 6 Abs. 1 lit. d DSGVO eine Verarbeitung rechtfertigen können, werden um den Zusatz ergänzt, dass dies nur gilt, wenn die betroffene Person außerstande ist, ihre Einwilligung zu geben.

Ein öffentliches Interesse kann nur noch dann eine Datenverarbeitung legitimieren, wenn die Verarbeitung in angemessenem Verhältnis zu dem verfolgten Ziel steht, der Wesensgehalt des Rechts auf Datenschutz gewahrt wird und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorgesehen sind. Dabei wird bewusst darauf verzichtet, das erhebliche Interesse aus Art. 9 Abs. 2 lit. g DSGVO zu übernehmen. Eine Übernahme würde nämlich dazu führen, dass lediglich besonders schützenswerte Interessen des Gemeinwohls als Rechtsgrundlage herhalten könnten, die mehr Gewicht haben als die Rechte der betroffenen Personen.[804] Beispiele dafür wären Krisen- und Konfliktbewältigung, Gefahrenabwehr für hochrangige, besonders schützenswerte Rechtsgüter oder humanitäre Maßnahmen.[805] In einem zusam-

801 *Kampert* (2018), Art. 9 Rn. 14; *Weichert* (2020), Art. 9 Rn. 47.
802 *Schiff* (2018), Art. 9 Rn. 33.
803 *Weichert* (2020), Art. 9 Rn. 47.
804 *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 16; *Schulz* (2018), Art. 9 Rn. 37; *Schiff* (2018), Art. 9 Rn. 52 ff.
805 *Schiff* (2018), Art. 9 Rn. 54; *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 16.

mengeführten System würden solche strikten Grenzen eine Behinderung vieler im öffentlichen Interesse liegender Verarbeitungstätigkeiten bedeuten. Demnach sollte die Anforderung an den notwendigen Grad des Interesses geändert werden. Nicht erforderlich ist ein „erhebliches" Interesse, sondern ein „ausreichendes". Dies würde bezwecken, dass öffentliche Interessen lediglich dann als Rechtsgrundlage für Verarbeitungen herhalten können, wenn eine gewisse Bedeutsamkeit erreicht wurde. Es muss somit nicht immer eine Krise oder Vergleichbares vorliegen, um ein öffentliches Interesse auszulösen und ebenso ist z.B. ein Stadtteil-Fest nicht genug, um Essgewohnheiten der Anwohner verarbeiten zu können, um die Essensversorgung zu planen. Ein ausreichendes öffentliches Interesse würde somit eine ausgewogene Balance zwischen erheblichen und völlig unbegrenzten Vorgaben ermöglichen. Durch die Hinzunahmen des weiteren Zusatzes aus Art. 9 Abs. 2 lit. g DSGVO würde dann ein sinnvoller und umfassender Reglungsrahmen geschaffen werden. Denn wenn für alle Verarbeitungen, die aufgrund eines öffentlichen Interesses stattfinden, gilt, dass diese in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person getroffen werden müssen, würde ein ausreichendes, allgemeines Schutzniveau erreicht werden. Hinzu kommt, dass der Gesetzgeber vorsieht, dass die Vorgaben zum öffentlichen Interesse unions- und/oder mitgliedsstaatsrechtlich ausgefüllt werden können.[806] Demnach wäre es möglich, weitere verschärfende Maßnahmen zu ergreifen, sollte in nachfolgenden Gesetzesevaluationen erkannt werden, dass kein ausreichender Schutz gewährleistet wird.

Art. 9 Abs. 2 lit. d, e, h DSGVO können ohne weitere Anpassungen in das neue System übernommen werden. Mit diesem neuen zusammengeführten Reglungsrahmen würden die steigenden Auswertungsmöglichkeiten von personenbezogenen Daten und die besondere Schutzbedürftigkeit von besonders sensitiven Daten ausreichend berücksichtigt werden. Ebenso würde damit keine deutlich strengere Regulierung etabliert werden, als sie derzeit unter Art. 6 DSGVO gilt. Die ökonomische Verwertung von Daten würde dadurch demnach nicht zwangsläufig beeinträchtigt sein.

Allerdings bestehen daneben noch zwei besondere Herausforderungen, die bislang nicht adressiert wurden: der Vertrag (Art. 6 Abs. 1 lit. b

806 *Spindler/Dalby* (2019), Art. 6 DSGVO Rn. 11; *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 16.

DSGVO) und das berechtigte Interesse (Art. 6 Abs. 1 lit. f DSGVO) bedürfen einer genaueren Betrachtung.

c. Der Vertrag als Rechtsgrundlage

Es könnte in Zukunft denkbar sein, dass Betroffene als Konsumenten die Überwachung ihrer Gehirnaktivitäten o.Ä. bei Unternehmen buchen und darüber einen Vertrag abschließen.[807] Ebenso ist es vorstellbar, dass z.B. Gehirnscans (und damit Wesensdaten) für bestimmte andere Vertragsabschlüsse verlangt werden. Es gibt derzeit bereits Verträge, bei denen vor Abschluss bestimmte sensitive Daten offengelegt werden müssen. Diverse Kauf- oder Finanzierungsgeschäfte sehen z.B. vor, dass der Käufer/Kunde seine Zahlungsfähigkeit nachweist. Es ist somit ebenso denkbar, dass in Zukunft auch Gehirnscans für den Abschluss von Verträgen notwendig werden könnten. Denkbar ist dies bspw. bei Geschäften, für die ein Nachweis von geistiger Stabilität notwendig ist. So sieht das deutsche Waffengesetz derzeit in § 4 Abs. 1 Nr. 2 WaffG i.V.m. § 6 Abs. 1 WaffG vor, dass es nur erlaubt ist eine Schusswaffe zu erwerben, wenn die Person u.a. psychisch stabil und verantwortungsvoll ist. Beide Voraussetzungen könnten mit BCI überprüft werden, indem z.B. neurologische Reaktionen auf bestimmte visuelle Reize ausgewertet werden. Damit die Legitimierung über einen Vertrag nicht missbraucht wird, um nach Belieben Wesensdaten zu verarbeiten, müssen die Vorgaben aus Art. 6 Abs. 1 lit. b DSGVO angepasst und um Sicherheitsmaßnahmen ergänzt werden.

Die Verarbeitung von personenbezogenen Daten sollte also weiterhin für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen möglich sein, solange dadurch keine wesentlichen Beeinträchtigungen der informationellen Selbstbestimmung der betroffenen Person ermöglicht werden. Dieser Zusatz könnte direkt im Gesetz verankert werden. Wobei unter „wesentliche Beeinträchtigungen der informationellen Selbstbestimmung" zu verstehen ist, wenn personenbezogene Daten mit großem Aussagepotential (z.B. aggregierte Schrittzahlen, die Aussagen über die Gesundheit der betroffenen Person machen können) und besonders intime Daten (z.B. explizite Patientenakten, die unmittelbar den Gesundheitszustand offenbaren) in großem Umfang verarbeitet werden sollen. Diese Definition sollte ergänzend in den Erwägungsgründen bereitgestellt werden.

807 *Ienca/Malgieri,* Journal of Law and the Biosciences 2022, S. 1 (14).

Das ergänzende Sicherheitskriterium des verbotenen, wesentlichen Eingriffs in die informationelle Selbstbestimmung macht es notwendig, dass vertraglich legitimierte Datenverarbeitungen genauer betrachtet werden müssen. Sobald die Erfüllung eines Vertrags oder die Durchführung von vorvertraglichen Maßnahmen als Legitimationsgrundlage für eine Datenverarbeitung dienen soll, bedarf es somit einer Prüfung, ob personenbezogene Daten mit großem Aussagepotential oder besonders intime Daten vorliegen und, ob diese Daten in großem Umfang verarbeitet werden sollen. Wenn dies der Fall ist, dann ist die geplante Datenverarbeitung nicht rechtmäßig.

d. Das berechtigte Interesse als Rechtsgrundlage

Die derzeitige Praxis zeigt, dass die schwierige Trennung zwischen personenbezogenen Daten und besonderen Kategorien personenbezogener Daten auch in Zukunft dazu führen könnte, dass Wesensdaten auf Grundlage des berechtigten Interesses verarbeitet werden können. Dies sollte allerdings tunlichst vermieden werden.

Um eine solche, missbräuchliche Anwendung des berechtigten Interesses zu vermeiden, sollten in einem zusammengeführten Regulierungssystem besondere Anpassungen vorgenommen werden. Grundsätzlich kann die derzeitige Formulierung aus Art. 6 Abs. 1 lit. f DSGVO allerdings beibehalten werden. Solange die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt, ist eine Verarbeitung somit gestattet. Dazu sollte jedoch ergänzend ein konkretisierender Absatz in den Art. 6 aufgenommen werden. Dieser sollte zum einen festlegen, dass die notwendige Interessenabwägung leicht verständlich und leicht zugänglich offengelegt werden muss, sobald die personenbezogenen Daten erhoben werden. Zum anderen sollte auch gefordert werden, dass die betroffene Person eindeutig und unmissverständlich darauf hingewiesen werden muss, wenn wesentliche Beeinträchtigungen ihrer informationellen Selbstbestimmung mittels des berechtigten Interesses ermöglicht werden. Abschließend sollten die Aufsichtsbehörden ebenso eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die das berechtigte Interesse ausgeschlossen ist. Verantwortliche haben diese Liste dann kontinuierlich zu berücksichtigen.

e. Eingliederung in die DSGVO

Das vorausgehend entworfene neue System könnte ohne großen Aufwand in die bestehende DSGVO eingegliedert werden. Dafür würde Art. 9 vollständig gestrichen und Art. 6 entsprechend ergänzt werden.

Art. 6 DSGVO würde dann wie folgt ausformuliert sein (Anpassungen sind in fett dargestellt):

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
   a. Die betroffene Person hat ihre **ausdrückliche** Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
   b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen, **solange dadurch keine wesentlichen Beeinträchtigungen der informationellen Selbstbestimmung der betroffenen Person ermöglicht werden.**
   c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt **und zur Einhaltung und Ausübung von Vorgaben aus dem Arbeitsrecht, Recht der sozialen Sicherheit und des Sozialschutzes sowie Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit nötig;**
   d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, **wenn die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;**
   e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im ausreichenden öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde **und, die in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht;**
   f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die

Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

g. die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemaligen Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

h. die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

i. die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Für die Rechtsgrundlage gemäß Absatz 1 lit. f gilt ergänzend:

a. die geforderte Interessenabwägung muss leicht verständlich und leicht zugänglich offengelegt werden, sobald die personenbezogenen Daten erhoben werden;

b. die betroffene Person muss eindeutig und unmissverständlich darauf hingewiesen werden, wenn wesentliche Beeinträchtigungen ihrer informationellen Selbstbestimmung mittels des berechtigten Interesses ermöglicht werden;

c. die Aufsichtsbehörde erstellt und veröffentlicht eine Liste der Verarbeitungsvorgänge, für die das berechtigte Interesse ausge-

schlossen ist und Verantwortliche haben diese Liste kontinuierlich zu berücksichtigen.

Alle weiteren bisherigen Vorgaben aus Art. 6 DSGVO (Abs. 2-4) könnten ohne weitere Anpassungen in das neue Regulierungssystem übertragen werden. In den Erwägungsgründen sollte an geeigneter Stelle lediglich noch ergänzt werden, dass eine wesentliche Beeinträchtigung der informationellen Selbstbestimmung vorliegt, wenn personenbezogene Daten mit großem Aussagepotential (z.B. aggregierte Schrittzahlen, die Aussagen über die Gesundheit der betroffenen Person machen können) und besonders intime Daten (z.B. explizite Patientenakten, die unmittelbar den Gesundheitszustand offenbaren) in großem Umfang verarbeitet werden sollen.

II. Eine neue Form der Einwilligung

Wie in Kapitel G.II.2 ausgeführt wurde, gibt es bei der derzeitigen Einwilligungspraxis zwei wesentliche Mängel. Erstens wird die gewünschte Informiertheit der Betroffenen in den meisten Fällen nicht erreicht und zweitens kann in vielen Fällen auch nicht von einer freiwilligen Einwilligung ausgegangen werden.

Damit die Einwilligung wieder zu einem verlässlichen Rechtsinstrument wird, ist eine zweigliedrige Herangehensweise notwendig. Erstens brauchen Verantwortliche klarere gesetzliche Vorgaben, wie die Informiertheit der betroffenen Personen hergestellt werden muss, und zweitens muss die Mündigkeit der betroffenen Personen in Bezug auf Datenschutz erhöht werden.

1. Eine neue Form der Einwilligung: gesteigerte Informiertheit

Um darzulegen, wie die Informiertheit der betroffenen Personen gesteigert werden könnte, ist eingehend eine kurze Auswertung der relevanten wissenschaftlichen Literatur notwendig. Wie bereits bei der Debatte um Warnungen auf Tabak-Erzeugnissen festgestellt wurde, erregen Texte allein kaum Aufmerksamkeit.[808] Etliche Studien haben gezeigt, dass Bilder oder

808 *Brennan et al.,* Nicotine & Tobacco Research 2017, S. 1138 (1138 ff.).

Animationen deutlich effektiver darin sind, das Interesse zu wecken.[809] Diese Tatsache sollte auch in der Kommunikation von rechtlichen Textern berücksichtigt werden,[810] besonders, weil die bildliche Kommunikation mittlerweile einen großen Stellenwert einnimmt und diesem Fakt Rechnung getragen werden muss.[811] Da das menschliche Gehirn aber dazu neigt, sich schnell an immer wiederkehrende Muster zu gewöhnen,[812] sind Animationen, auch wenn nur simpel und klein, im digitalen Kontext zu bevorzugen. Förderlich ist es ebenso, wenn die notwendige Datenschutzerklärung standardgemäß vor einer Einwilligung tatsächlich angezeigt und nicht nur verlinkt wird o.Ä., da damit die Wahrscheinlichkeit steigt, dass Betroffene diese auch lesen.[813] Doch damit das Gelesene auch verstanden wird, bedarf es ergänzend einer prägnanten und verständlichen Informationsvermittlung. Um dies zu erreichen, ist es notwendig, auf das durchschnittliche Leseverständnis in der Europäischen Union abzustellen. Laut der Bewertungsskala der Organisation for Economic Co-operation and Development (OECD) liegt das durchschnittliche europäische Leseverständnis bei ca. 269 von 500 möglichen Punkten.[814] Das bedeutet, dass der durchschnittliche Mensch mittellange, nicht allzu anspruchsvolle Texte, Darstellungen (Tabellen, Grafiken, etc.) oder Texte inklusive Darstellungen grundlegend verstehen, wichtige Informationen identifizieren und simple Schlüsse ziehen kann.[815] Dies unterstreicht die Notwendigkeit, dass Datenschutzerklärungen kürzer und weniger komplex gehalten werden sollten, damit eine durchschnittliche Verständlichkeit gewährleistet ist.[816] Allerdings darf die notwendige Kürze nicht dazu führen, dass einige Tatsachen, die ggf. trivial oder bereits bekannt erscheinen, ausgelassen werden und somit die Informiertheit der betroffenen Person untergraben wird.[817] Da eine vollständige

809 *Ditai et al.,* Trials 2018, S. 1 (5 ff.); *Pratt et al.,* Psychological Science 2010, S. 1724 (1724 ff.); *Tabassum et al.,* Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 2018, S. 1 (1 ff.).

810 *Boehme-Neßler,* Pictoral Law, 2011, S. 126 f.

811 *Boehme-Neßler,* Pictoral Law, 2011, S. 115 f.

812 *Anderson et al.,* ICIS 2014 Proceedings 2014, S. 1 (1 ff.).

813 *Bravo-Lillo et al.,* Proceedings of the Ninth Symposium on Usable Privacy and Security 2013, S. 1 (1 ff.); *Steinfeld,* Computers in Human Behavior 2016, S. 992 (992 ff.).

814 *OECD,* Skills Matter: Additional Results from the Survey of Adult Skills, 2019, S. 46.

815 Ebenda, S. 43.

816 Auswertung zu Lesbarkeit und Verständlichkeit von Informationen zur Teilnahme an medizinischen Covid-19 Impfstudien kam zum gleichen Schluss: *Emanuel/Boyle,* JAMA Network Open 2021, S. 1 (2 f.).

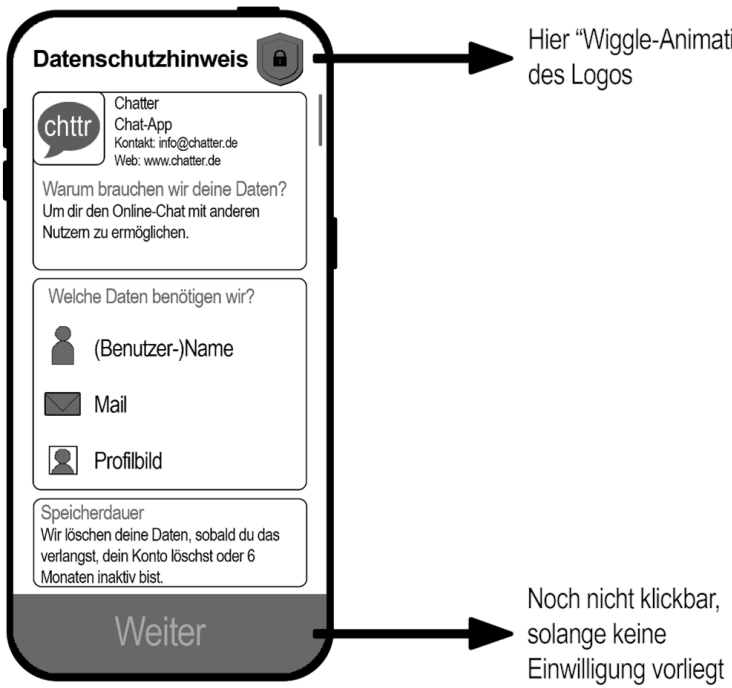
817 *Gluck et al.,* Proceedings of the Twelfth Symposium on Usable Privacy and Security 2016, S. 321 (323 ff.).

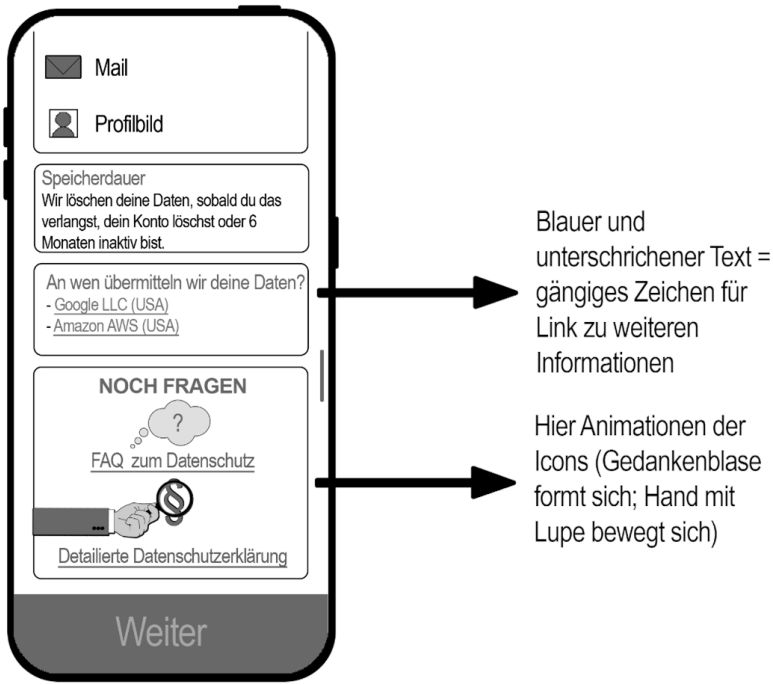
Information über die Datenverarbeitung meist nicht mit einer deutlich kürzeren Form vereinbar ist, bietet es sich an, dass der betroffenen Person standardgemäß nur die wichtigsten, für die Entscheidung relevanten Informationen als prägnante Aufzählung präsentiert werden. Die wichtigen, für die Entscheidung relevanten Informationen sind somit nicht alle geforderte Angaben nach Art. 13 u. 14 DSGVO, sondern nur eine Auswahl dieser. Um eine informierte Entscheidung zu ermöglichen, sollten mindestens der Verantwortliche (Art. 13 Abs. 1 lit. a DSGVO), die Verarbeitungszwecke (Art. 13 Abs. 1 lit. c DSGVO), die betroffenen personenbezogenen Daten (Art. 14 Abs. 1 lit. d DSGVO), die Empfänger bzw. Kategorien der Empfänger inkl. Länderstandort (Art. 13 Abs. 1 lit. e u. f DSGVO) und die Speicherdauer der Daten (Art. 13 Abs. 2 lit. a DSGVO) in der prägnanten Aufzählung enthalten sein. Die ausführliche Datenschutzerklärung könnte als Link oder weitere Handreichung bei Interesse zugänglich gemacht werden. Dies würde die durchschnittliche Informiertheit der Betroffenen erhöhen.[818] Damit diese Informiertheit auch in eine zielführende bestätigende Handlung überführt werden kann, bedarf es Mechanismen, die eine einfache Interaktion ermöglichen. Dabei sollten besonders im digitalen Bereich Designs und Mechanismen verwendet werden, die bereits etabliert sind. Besonders die Methoden „Drag and Drop" und „Swiping" fördern die Interaktion und sind den meisten Nutzern schon bekannt.[819]

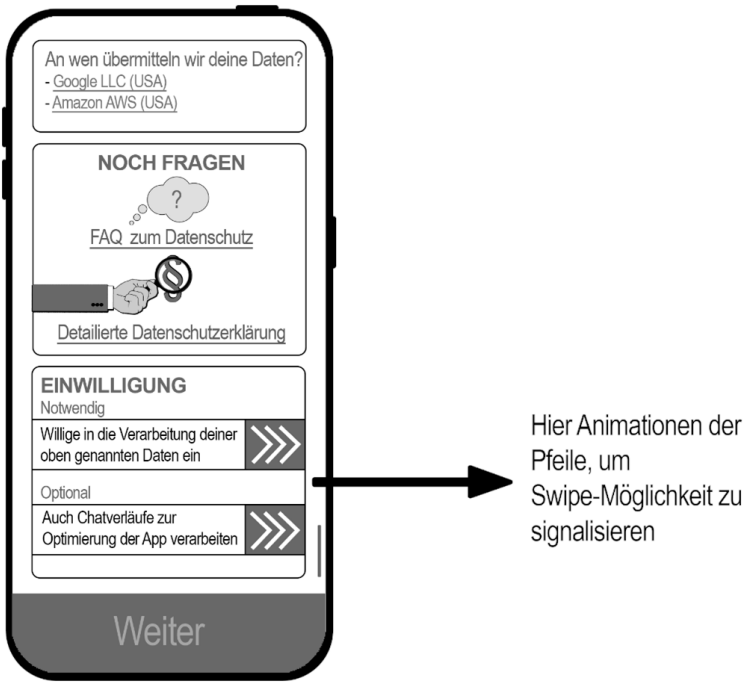
Aus der Auswertung der relevanten wissenschaftlichen Literatur geht demnach hervor, dass für eine informierte Einwilligung drei Aspekte notwendig sind: 1. Aufmerksamkeit/Interesse, 2. prägnante und verständliche Informationsvermittlung und 3. einfache und zielführende Interaktion. Unter Berücksichtigung dieser drei Punkte könnte eine angepasste Version des datenschutzrechtlichen Einwilligungsmechanismus, der die Informiertheit bestmöglich gewährleistet, bspw. wie folgt aussehen:

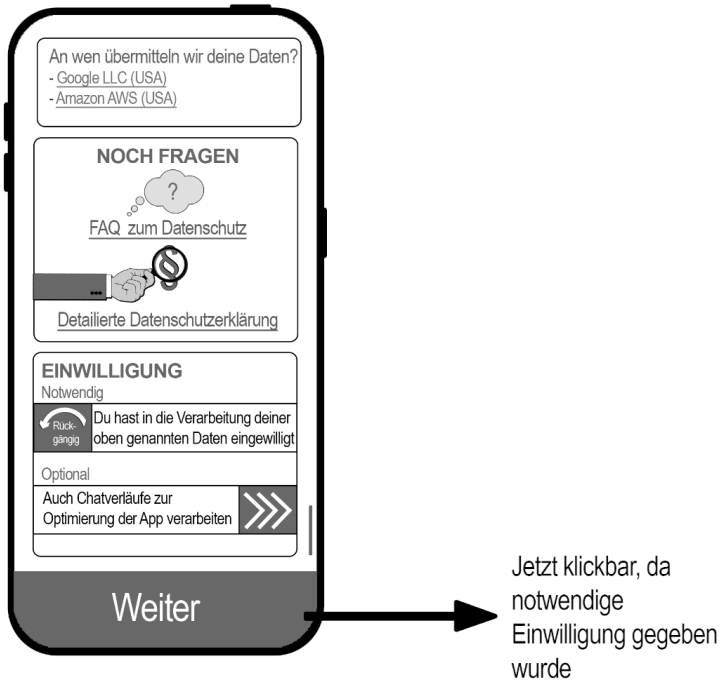
818 *Bergram et al.,* ECIS 2020 Research Papers 2020, S. 1 (1 ff.).
819 *Lindegren et al.,* Behaviour & Information Technology 2019, S. 398 (406 ff.).

Abbildung 2: Mögliche Gestaltung eines Einwilligungsmechanismus, der die Informiertheit der Betroffenen erhöht.









Um eine übersichtliche Darstellung präsentieren zu können, wurde hier bewusst ein sehr simples Beispiel gewählt. Nichtsdestotrotz kann das Prinzip auch für umfangreichere Datenschutzerklärungen und Einwilligungen genutzt werden. Allerdings würde man auch mit diesem Vorgehen nicht erreichen, dass alle betroffenen Personen die notwendigen Informationen erhalten, die sie brauchen, um eine informierte Einwilligung abzugeben. Denn letztendlich liegt der Umgang mit der datenschutzrechtlichen Einwilligung zu einem gewissen Grad auch in der Selbstverantwortung der Nutzer. Diese könnte wiederum durch eine weitere Sensibilisierung der Bevölkerung in Bezug auf Datenschutz gesteigert werden, wodurch betroffene Personen ggf. dazu ermutigt werden, noch weitere ergänzende Maßnahmen zu ergreifen.[820] Jedoch gewährleistet das hier ausgearbeitete Modell eine vergleichsweise niedrigschwellige Möglichkeit der Informationsvermittlung, mit der mehr Betroffene erreicht werden könnten als bislang. Somit ist davon aus-

820 Bspw. könnten Betroffene KI-Tools nutzen, die Datenschutzerklärungen auf Vollständigkeit überprüft o.ä.: *Torre et al.,* IEEE 28th International Requirements Engineering Conference (RE) 2020, S. 136 ff.

zugehen, dass im Vergleich zu den oben genannten Zahlen signifikant mehr Menschen durch diesen Einwilligungsmechanismus informierte Entscheidungen treffen werden.

2. Eine neue Form der Einwilligung: gesteigerte Freiwilligkeit

Wesentlicher Punkt bei der datenschutzrechtlichen Einwilligung ist ergänzend noch die Freiwilligkeit der Willensbekundung. Wie bereits dargelegt, haben viele Menschen das Gefühl, dass sie den Datenschutzerklärungen sowieso zustimmen müssen, wenn sie den Dienst nutzen wollen.[821] Dies ist ein maßgeblicher Grund für das sog. Privacy Paradoxon, bei dem der Schutz von personenbezogenen Daten und der Privatsphäre zwar als wichtig eingestuft wird, aber nicht zwangsläufig das Verhalten der Nutzer bestimmt.[822] Vielmehr wird die erhaltene Leistung, die oftmals auf der Preisgabe von Daten basiert, als größerer Vorteil eingestuft, als der Erhalt der Privatsphäre.[823] Erschwerend kommt hinzu, dass die deutschen Internetnutzer größtenteils Angst vor dem Kontrollverlust über ihre Daten haben und kaum wissen, was sie selbst unternehmen können, um ihre Daten besser zu schützen.[824]

Auch hier ist vor allem auf die Selbstverantwortung der betroffenen Personen abzustellen. Jeder Person ist es selbst überlassen, ob sie Dienste nutzt, für die sie mit ihren personenbezogenen Daten bezahlen muss. Es kann durchaus argumentiert werden, dass sich die Nutzung von Social Media, Smartphones, Apps, etc. zu einem essenziellen Bestandteil des modernen Lebens entwickelt hat, womit sich viele Personen demnach indirekt dazu gezwungen fühlen diese Dienste zu nutzen, um nicht vom gegenwärtigen gesellschaftlichen Leben ausgeschlossen zu werden, auch wenn damit die persönliche Privatsphäre eingeschränkt wird. Dies macht deutlich, dass eine mögliche Korrelation zwischen der Angst, etwas zu verpassen,[825] und der mangelnden Kenntnis über datenschutzfreundliche und vergleichbare Alternativen zu den etablierten Anbietern besteht. Diese Kenntnis kann bspw. durch gesellschaftliche Sensibilisierung erreicht werden und durch gesteigerte diesbezügliche Selbstverantwortung. Es gibt bereits etliche da-

821 N*iedermann,* Allensbacher Archiv 2019, S. 1 (7).
822 *Engels,* IW-Trends 2018, S. 3 (6).
823 *Engels/Grunewald,* IW-Kurzberichte 2017 (57), S. 1 (1).
824 *Bitkom,* Datenschutz in der digitalen Welt, 2015, S. 3.
825 *Przybylski et al.,* Computer in Human Behavior 2013, S. 1841 (1842).

tenschutzfreundliche Alternativen zu populären datengetriebenen Diensten, womit es vor allem an der Mündigkeit der betroffenen Personen liegt, sich vom Privacy Paradoxon zu befreien. Ebenso ist davon auszugehen, dass die erhaltene Leistung, die meist auf der Preisgabe von Daten basiert, oftmals nur als größerer Vorteil eingestuft wird als der Erhalt der Privatsphäre, da die Betroffenen nicht ausreichend über die Datenverarbeitung informiert wurden und darum eine ungenaue individuelle Risikoabschätzung vornehmen.

Damit die betroffenen Personen dieser Selbstverantwortung vollumfänglich gerecht werden können, bedarf es ergänzend ebenso striktere Vorgaben für Verantwortliche denn oftmals verwenden diese bewusst sog. Dark Patterns.[826] Dark Patterns sind bspw. Elemente von Einwilligungs-Tools auf Internetseiten, die so gestaltet werden, dass Nutzer dazu verleitet werden, einzuwilligen, obwohl sie dies eigentlich gar nicht wollen.[827] Bereits 2019 verbot der EuGH eine Form von Dark Patterns, indem vorausgefüllte Einwilligungen, die nicht aktiv von den Betroffenen gegeben wurden, als rechtswidrig eingestuft wurden.[828] Allerdings bestehen noch etliche weitere solcher Mechanismen, die die Freiwilligkeit der Betroffenen untergraben können. Ein klares Signal wäre hier das grundsätzliche Verbot von Dark Patterns.[829] Dabei sollte das Verbot so formuliert werden, dass deutlich wird, ab wann Gestaltungselemente als Dark Patterns einzustufen sind und ab wann diese nicht mehr DSGVO-konform sind. Denkbar wäre darum folgende Ergänzung zu Art. 7 Abs. 4 DSGVO (vorgeschlagene Ergänzung in fett):

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde**, ist maßgeblich, ob Techniken eingesetzt wurden, die die betroffenen Personen unbewusst zu für sie unvorteilhaften Entscheidungen verleiten**. Ebenso muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

826 *Machuletz/Böhme,* Proceedings in Privacy Enhanching Technologies 2020, S. 481 (481 ff.); *Nouwens et al.,* Proceedings oft he 2020 CHI Conference in Human Factors in Computing Systems 2020, S. 1 (1 ff.).

827 *Forbrukerrådet,* Deceived by Design, 2018, S. 6 f.

828 EuGH, Urt. v. 1.10.2019 – (Planet49), ZD 2019, 556.

829 In den USA gab es dazu bereits einen Gesetzesentwurf: *Warner/Fisher*: Deceptive Experiences To Online Users Reduction (DETOUR) Act, 2019.

III. Technischer Datenschutz: Allgemeine Verpflichtung notwendig

Es wurde bereits ausgeführt, dass sich nach derzeitiger Formulierung des Art. 32 u. Art. 25 DSGVO nur Verantwortliche an die Pflicht zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen halten müssen. Wie allerdings festgestellt wurde, ist dies in Bezug auf die zukünftige Verarbeitung von Wesensdaten nicht unbedingt förderlich, weswegen eine allgemeine Verpflichtung zu bevorzugen ist.

Bei BCI handelt es sich um eine noch neue bzw. junge Technologie. Für Verantwortliche steht derzeit nur eine begrenzte Anzahl an Herstellern zur Auswahl. Um die Verpflichtung zum Datenschutz durch Technikgestaltung einzuhalten, sind Verantwortliche demnach nochmal mehr auf die Hersteller/Entwickler angewiesen. Aus Gründen, die vorausgehend bereits dargelegt wurden, ist davon auszugehen, dass besonders zu Beginn der initialen Verbreitung der neuen Technologie nicht sofort datenschutzfreundliche Alternativen zur Verfügung stehen werden. Für Anbieter von BCI wird der Fokus wahrscheinlich auf der Bereitstellung der versprochenen Funktionalitäten und der schnellen Markterschließung liegen und nicht auf Datenschutz.

Um die grundlegenden Probleme beim Datenschutz durch Technikgestaltung zu lösen und um einen ganzheitlich sicheren Umgang mit Wesensdaten zu gewährleisten, ist eine mittelbare Verpflichtung von Herstellern/Entwicklern demnach nicht geeignet. Ohne die Verpflichtung zu Datenschutz durch Technikgestaltung direkt an der Wurzel, wird Datenschutz nicht die Priorisierung erhalten, die notwendig und auch gewünscht ist. Besonders bei der zukünftigen Verarbeitung von hoch sensitiven Wesensdaten sollten bereits bei der Entwicklung der Technologie Maßnahmen berücksichtigt werden, die bestmöglichen Datenschutz gewährleisten. Grundsätzlich ist somit zu empfehlen, von der alleinigen Verpflichtung von Verantwortlichen abzuweichen und zu einer allgemeinen Notwendigkeit von Datenschutz durch Technikgestaltung zu wechseln.