Oldenburger Forum der Rechtswissenschaften

Maurice Matthijs Oettel Ziebell

Smart Human und der Schutz der Gedanken

Die europäische Datenschutz-Grundverordnung im Zeitalter von Brain-Computer-Interfaces

Nomos

Oldenburger Forum der Rechtswissenschaften

Schriftenreihe des Instituts für Rechtswissenschaften
der Carl von Ossietzky Universität

Herausgegeben von
Professor Dr. Dr. Volker Boehme-Neßler
Professor Dr. Christiane Brors
Professor Dr. Christine Godt

Band 12

Maurice Matthijs Oettel Ziebell

Smart Human und der Schutz der Gedanken

Die europäische Datenschutz-Grundverordnung im Zeitalter von Brain-Computer-Interfaces

Nomos

Diese Veröffentlichung wurde aus Mitteln des Publikationsfonds NiedersachsenOPEN, gefördert aus zukunft.niedersachsen, unterstützt.

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

Zugl.: Oldenburg, Univ., Diss., 2025

1. Auflage 2026

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-4322-4
ISBN (ePDF): 978-3-7489-7183-2

DOI: https://doi.org/10.5771/9783748971832

Onlineversion
Inlibra

Diese Arbeit widme ich all denen, die ich liebe,
und all denen, deren Liebe ich empfangen darf:
meinen Eltern, meinen Geschwistern, meinen Freunden
und ganz besonders Franni.

Großer Dank gilt meinem Doktorvater,
Prof. Dr. Dr. Volker Boehme-Neßler, für seinen Einsatz und
seine Unterstützung. Ohne sein Zutun wäre diese Arbeit
wahrscheinlich niemals entstanden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BCI	Brain Computer Interface
DDoS	Distributed-Denial-of-Service
DDR	Deutsche Demokratische Republik
DoS	Denial-of-Service
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
EEG	Elektroenzephalogramm
ErwG	Erwägungsgrund
fMRT	Magnetresonanztomographie
GG	Grundgesetz
GRCh	Charta der Grundrechte der Europäischen Union
IoT	Internet of Things
KI	Künstliche Intelligenz
MEG	Magnetenzephalographie
NIS	Nahinfrarotspektroskopie
PC	Personal Computer

A. Smart Human

Das Verständnis und die Wahrnehmung von Menschsein befindet sich in ständigem Wandel. Es wird dabei von allgemeinen kulturellen Strömungen beeinflusst. Die derzeit relevanteste Einflussgröße auf das Verständnis und die Wahrnehmung von Menschsein dürfte die Technisierung sein. Der damit einhergehende Umgang mit Technik ist vor allem durch eine zunehmende Vermenschlichung geprägt. Diese beiden Aspekte – Technisierung und die Vermenschlichung von Technik - bedingen nun eine technologische Entwicklung, die das Verständnis von Menschsein in Zukunft wesentlich verändern dürfte.

I. Technisierung

1. Ein Deutungsversuch

Die grundsätzliche Verbindung zwischen Menschen und Technologie wird zunehmend intensiver und umfassender. Es kennzeichnet unsere Moderne, dass die Technisierung mittlerweile in jeden Lebensbereich Einzug gehalten hat. Was genau unter Technisierung zu verstehen ist, ist allerdings unklar.

Das zugrunde liegende Wort „Technik" kommt vom griechischen Wort téchne (τέχνη), was Geschick, Kunstfertigkeit oder auch Kunst bedeuten kann. Es bezeichnet somit das bereichsübergreifende Können des Menschen, etwas herzustellen.[1] Rein etymologisch ist Technik also alles, was durch das Geschick oder durch die Kunstfertigkeit des Menschen geschaffen wurde. Die weite Auslegung des Technikbegriffs greift dies auf und besagt, dass jedes zweckgerichtete, planvoll und rational genutzte Mittel sowie das konkrete Handeln des Menschen mit Hilfe dieser Mittel, als Technik zu definieren sei.[2] Im Gegensatz dazu besteht aber auch eine enge Auslegung des Technikbegriffs aus der konkreten Technikwissenschaft. Hier wird nur das künstliche Artefakt an sich, die Maschine, der Gegenstand, als Technik

1 *Meyer,* Die Technisierung der Welt, 1961, S. 9.
2 *Weber,* Wirtschaft und Gesellschaft, 1921, S. 32.

bezeichnet – losgelöst von den menschlichen Zwecken und Zielen.[3] Beide Herangehensweisen vernachlässigen jedoch jeweils eine Dimension des Technikbegriffs, entweder das Menschliche oder das Gegenständliche. Am treffendsten ist somit eine symbiotische Deutung, die die beiden Auffassungen zusammenführt. Technik sind nach einer solchen Auslegung zweck-/nutzenorientierte und von Menschen gefertigte künstliche Gegenstände.[4] Technisches Handeln kann dabei als Herstellung oder Nutzung dieser Gegenstände auftreten.[5]

Ausgehend von diesem Verständnis des Technikbegriffs, kann auch Technologisierung als solches erschlossen werden. Das Suffix „-ierung" des Wortes dient als mögliche Substantivierung von Verben mit „-ieren"-Endung. Das zugrunde liegende Verb für diese Substantivierungen ist demnach „technisieren". Die Endung „-ierung" ist meist ein Anzeichen dafür, dass eine Handlung oder ein Vorgang gemeint ist.[6] Daraus lässt sich bereits schließen, dass mit Technisierung etwas noch nicht Vollendetes bezeichnet wird. Der Begriff Technik ist in diesem Gefüge der Wortstamm und legt somit auch die grundlegende Bedeutung fest. Geht man nun vom vorherig präsentierten Verständnis von Technik aus, ist das Verb ‚technisieren' die aktive Herstellung und Nutzung von nutzenorientierten, von Menschen gefertigten künstlichen Gegenständen. Daraus resultiert zwangsläufig, dass beim Technisieren die Menge der künstlichen Gegenstände und die Menge der menschlichen Handlungen, bei denen diese Gegenstände erstellt und verwendet werden, kontinuierlich wächst. Technisierung beschreibt demnach den daraus resultierenden Vorgang, also den Prozess, bei dem Technik durch Technisieren umgesetzt wird. Technisierung kann also definiert werden als kontinuierliche Steigerung der vorhandenen nutzenorientierten, künstlichen Gegenstände und der menschlichen Handlungen, in denen diese Gegenstände entstehen oder verwendet werden.

3 *Dessauer*, Philosophie der Technik, 1927, S. 7.
4 *Ropohl*, Allgemeine Technologie, 2009, S. 30.
5 *Tuchel,* Herausforderung der Technik, 1967, S. 23ff.
6 Abrufbar unter: https://www.duden.de/rechtschreibung/_ation__ierung (abgerufen 6.4.2022).

2. Einschlägige Beispiele für Technisierung

a. Internet of Things

Ein beeindruckendes aktuelles Beispiel für die Technisierung ist das sog. Internet of Things (IoT). IoT zeichnet sich dadurch aus, dass zunehmend smarte Geräte ans Internet angeschlossen und dort auch verwaltet werden und sich somit zu einem Geflecht von Dingen zusammenfügen, deren Mittelpunkt der Nutzer und seine Handlungen sind.[7] Dies kann deutlich als kontinuierliche Steigerung der nutzenorientierten und künstlichen Gegenstände sowie der menschlichen Handlungen, mit denen diese Gegenstände verwendet werden, verstanden werden. Ein solches Netz an Geräten kann viele Vorteile haben. So können vernetzte Maschinen bspw. Smart Factories bilden, womit potenziell Unfälle oder Risiken für die Arbeiter minimiert werden könnten.[8] Im Zuge von Smart Cities ist das IoT wesentlich, um Daten zu sammeln und zu analysieren, um ggf. nachhaltigere Städte zu ermöglichen.[9]

Auf der anderen Seite kann das IoT auch eine Gefahr darstellen. Es kann bspw. dazu missbraucht werden, um individuelle und umfassende personenbezogene Datensphären zu erschaffen,[10] die nicht nur die Privatheit reduzieren, sondern auch das Potential haben, eine ernstzunehmende Bedrohung für die Freiheit der Nutzer darzustellen.[11] Solche Datensphären erhöhen auch die Gefahr von unbefugtem Zugang zu den Informationen oder unbefugter Offenlegung der Daten.[12] Demnach ist ein bedachter Umgang mit dem IoT notwendig.[13]

---

7 *International Telecommunication Union,* Overview of the Internet of Things, 2013, S. 2 f.; *Al-Taair/Kanber/al-Dulaimi,* International Journal of Emerging Technologies in Learning 2023, S. 19 (21).

8 *Soori/Arezoo/Dastres,* Internet of Things and Cyber-Physical Systems 2023, S. 192 (198).

9 *Ullah et al.,* Complex & Intelligent Systems 2024, S. 1607 (1610 ff.).

10 *Hofmann/Hornung,* in: Sprenger/Engemann, Internet der Dinge, 2015, S. 181 (194).

11 *Adamowsky,* in: Sprenger/Engemann, Internet der Dinge, 2015, S. 119 (121).

12 *Rodrígues/Otero/Canal,* Sensors 2023, S. 1 (6 ff.).

13 Es gibt derzeit bereits Bemühungen das IoT anonym oder privater zu gestalten, einen guten Überblick dazu bieten: *Rodrígues/Otero/Canal,* Sensors 2023, S. 1 (5 ff.); *Neves et al.,* Journal of Computer Security 2023, S. 261 (261 ff.).

b. Human Enhancement, Transhumanismus und Posthumanismus

Mit dem Human Enhancement bahnt sich nach dem IoT eine weitere umfassende Technologisierung an. Bei Human Enhancement handelt es sich um die gezielte Optimierung von menschlichen Gegebenheiten, die über die natürlichen Grenzen und Maßstäbe hinausgeht.[14] Getrieben von der transhumanistischen Maxime, die derzeit bestehenden Limitationen des menschlichen Körpers und Lebens zu beseitigen,[15] steht dabei die Überwindung des Alterns und der mentalen Grenzen an zentraler Stelle.[16] Ziel des transhumanistischen Human Enhancements ist es, den derzeitigen Stand der menschlichen Spezies hinter sich zu lassen und die Transzendenz des Menschlichen zu erreichen,[17] zum Zwecke einer gelenkten Evolution in Richtung Super-Spezies, zur individuellen Weiterentwicklung oder aber zum Wohle der Gesellschaft.[18] Dies hätte den Posthumanismus zur Folge, bei dem Menschen mithilfe von Technologie zu etwas ganz Neuem, nicht mehr Menschlichem werden.[19]

Nicht unbedingt transhumanistisch bzw. posthumanistisch motiviert, aber doch mit dem medizinischen Ziel, die Limitationen des menschlichen Körpers zu überwinden, finden sich schon derzeit etliche Technologien, die in den menschlichen Körper implantiert werden. Beispielhaft ist hier vor allem der bereits gängige Herzschrittmacher zu nennen, der Herzkrankheiten ausgleichen oder mildern kann und damit die Lebenserwartung von Betroffenen drastisch erhöht.[20] Auch in der Neuro-Technologie bestehen bereits weitverbreitete implantierbare Geräte. Hier ist besonders das Cochlear-Implantat hervorzuheben, welches mit den Neurorezeptoren im Innenohr interagiert, um die beeinträchtigte oder nichtvorhandene Funktion der Gehörschnecke bei gehörlosen Personen zu ersetzen.[21]

---

14 *Erden/Brey,* Artificial Organs 2023, S. 1235 (1236); *Woyke,* in: Woyke et al., Die Debatte über „Human Enhancement", 2010, S. 21 (21 f.).
15 *Battle-Fisher,* Ethics, Medicine and Public Health 2020, S. 1 (2); *Brusseau,* Discover Artificial Intelligence 2023, S. 1 (3 f.).
16 *Nyholm,* Cambridge Quarterly of Healthcare Ethics 2023, S. 76 (80 ff.); *Lilley,* Transhumanism and Society, 2013, S. 1 f.
17 *Battle-Fisher,* Ethics, Medicine and Public Health 2020, S. 1 (2).
18 *Lilley,* Transhumanism and Society, 2013, S. 14 ff.
19 *Brusseau,* Discover Artificial Intelligence 2023, S. 1 (3 f.).
20 *Clément*, Brain-Computer Interface Technologies, 2019, S. 7.
21 Ebenda, S. 69 ff.

II. Vermenschlichung

Ein besonderer Aspekt der Technisierung ist die Vermenschlichung. Diese zeigt sich z.B. bei smarten Geräten. Smarte Geräte sind aus dem modernen Dasein nicht mehr wegzudenken. Das Smart Home ist mit Smart TV, Smart Light und Smart Speakern ausgestattet und in der Garage wartet das Smart Car. Die Bezeichnung „smart" verdeutlicht schnell, was von diesen Geräten gehalten wird. Der Begriff ist positiv konnotiert, er kreiert die Vorstellung von etwas Durchdachtem, etwas Klugem. Dem Gerät wird eine eigentlich menschliche Eigenschaft zugeschrieben, wodurch es einfacher wird, auf dessen Funktionen und Integrität zu vertrauen.

Die Tendenz Nicht-Menschliches zu vermenschlichen ist nichts Neues. Die allgemeine und wissenschaftliche Auseinandersetzung mit Tieren und deren Emotionen sowie Verhaltensweisen ist bspw. oftmals von einer solchen Anthropomorphisierung geprägt.[22] Das Gleiche gilt auch bei Robotern und KI-Systemen. Untersuchungen zeigen, dass die Ausgestaltung und das Design von Robotern und KI-Systemen wesentlichen Einfluss darauf haben kann, ob diese eine vermenschlichende Reaktion bei Nutzern auslösen.[23] Ein solcher Anthropomorphismus ist nicht verwunderlich, da die einzige bewusste Erfahrung, die der Mensch kennt, schließlich seine eigene ist.[24] Es ist somit nicht ungewöhnlich, dass menschliche Attribute nicht-menschlichen Entitäten zugeschrieben werden, sodass z.B. technische Geräte unter bestimmten Umständen als „smart" gelten können. Das Wort „smart" ist demnach zu etwas geworden, das nicht mehr alleinig Menschen beschreibt. Der Begriff hat sich vielmehr vom alleinig Menschlichen gelöst und wurde ebenso zu einer gängigen technischen Spezifikation.

Diese Tendenz des Anthropomorphismus birgt allerdings Herausforderungen und Gefahren. Wenn menschliche Gegebenheiten als Blaupause genutzt werden, um nicht-menschliche Gegebenheiten zu beschreiben, wird im Endeffekt tatsächlicher Erkenntnisgewinn erschwert.[25] Nicht-menschli-

22 *Humphreys*, Animals, Ethics, and Language, 2023, S. 12 ff.

23 *Kim/Im,* Computers in Human Behavior 2023, S. 1 (1 ff.): zeigen bspw., dass körperlose hohe Intelligenz menschlicher wahrgenommen wird als hohe Intelligenz mit schlecht designter körperlicher Erscheinung; *Phillips et al.*, HRI `18: Proceedings oft he 2018 ACM/IEEE International Conference on Human-Robot Interaction 2018, S. 105 (109 ff.): Zeigen, welche Merkmale bei Robotern eher zu einer Vermenschlichung führen – der größte Einfluss hat der sog. „Surface Look" (Geschlecht, Haut, Gesicht).

24 *Nagel,* The Philosophical Review 1974, S. 435 (438 ff.).

25 *Williams/Brosnan/Clay,* Neuroscience & Biobehavioral Reviews 2020, S. 299 (301 f.).

che Verhaltensweisen nur anhand von menschlichen Erfahrungswerten zu interpretieren, könnte die Realität verzerren oder verfehlen.[26] Ebenso kann eine Vermenschlichung dazu führen, dass nicht-menschlichen Entitäten mehr Vertrauen und Zurechnungsfähigkeit zugesprochen wird, als dies gerechtfertigt wäre. KI-Systeme oder Roboter, die eine anthropomorphisierende Reaktion bei Nutzern auslösen, könnten somit dazu verleiten, persönlichere Verbindungen mit ihnen einzugehen und mehr Informationen mit diesen zu teilen.[27]

III. Technisation und Metamorphose

Die allgemeine Technisierung und die damit einhergehende Vermenschlichung könnte nun einen wesentlichen Wendepunkt erreichen. Die Technisierung ist mittlerweile so weit fortgeschritten, dass so ziemlich jeder Lebensbereich von Technik durchdrungen ist. Kommunikation, Unterhaltung, Produktion, Verkehr, Bildung und Weiteres ist ohne Technologie kaum noch realisierbar.

Mit sog. Brain-Computer Interfaces (BCI) wird nun der nächste Schritt vollzogen. BCI ermöglichen die Aufzeichnung von Gehirnströmen, damit eine künstliche Intelligenz (KI) diese übersetzen und entweder passiv auswerten oder in aktive Handlungen umwandeln kann. Dies wird entweder durch ein externes Modul, wie z.B. ein Elektroenzephalogramm (EEG), oder aber durch einen chirurgisch ins Gehirn implantierten Chip gewährleistet,[28] womit eine Verknüpfung des menschlichen Nervensystems mit einem elektronischen System, wie bspw. einem Computer, erreicht wird.[29] Die zukünftigen Anwendungsmöglichkeiten von BCI sind damit weitreichend und nicht nur auf den medizinischen Bereich beschränkt. Das

26 *Samhita/Gross,* Communicative & Integrative Biology 2013, S. 1 (1 ff.): Beschreiben den Fall vom „Cleveren Hans", einem Pferd, welches scheinbar Rechenaufgaben lösen konnte, indem es Zahlen/Antworten mit der Hufe klopfte. Es stellte sich jedoch heraus, dass das Pferd vielmehr in der Lage war mikroskopische Signale in den Gesichtern der Menschen zu lesen, aufgrund dessen dann die richtige Antwort gegeben wurde.

27 *Kronemann et al.,* Spanish Journal of Marketing 2023, S. 3 (13); *Chi/Vu*, CAAI Transactions on Intelligence Technology 2023, S. 260 (269 f.): Zeigen jedoch, dass Vertrauen in KI nicht nur durch Vermenschlichung erreicht werden kann, da Angst vor der Technologie wahrscheinlich auch eine Rollen spielt.

28 *Guger et al*., in: Guger et al., Brain-Computer Interface Research, 2019, S. 1 (1).

29 *Clément*, Brain-Computer Interface Technologies, 2019, S. 1.

Steuern von Geräten per Gedanke, Gedankenübertragung und die digitale Einspeisung von Informationen direkt in das Gehirn sind denkbar.

Die Entwicklung auf dem Gebiet der BCI erweitert das transhumanistische/posthumanistische Human Enhancement deutlich und führt dazu, dass die Technisierung nun auch das Wesen des Menschen erreicht, seinen Geist. Aus Technisierung wird damit Technisation. Die beiden Wortendungen „-ierung" und „-ation" können sich geringfügig in ihrer Bedeutung unterscheiden. Während Wörter mit dem Suffix „-ierung" die Handlung oder den Vorgang an sich darstellen, beschreibt die Wortendung „-ation" eher das Resultat einer Handlung. Technisierung liegt also nur so lange vor, bis die Technisation erreicht ist. Technisation ist dabei die vollständige und umfassende Durchdringung einer Gesellschaft, deren Kultur und deren Menschen durch Technik. BCI haben somit das Potenzial, ein fundamentales Überdenken des Menschlichen anzustoßen.

Neben der Technisierung dürfte die Vermenschlichung ebenso wesentlich dazu beitragen, dass die Verbindung zwischen Menschen und Technik immer stärker wird. Chattende KI-Systeme, reagierende Sprachassistenten und Roboter mit menschlichem Körperbau und Aussehen, machen Vertrauen einfacher und Abhängigkeiten hinnehmbarer.

Durch BCI findet aber eine interessante Umkehrung der Vermenschlichung statt. Denn nun trifft die Vermenschlichung wieder auf den Menschen und führt zur Entmenschlichung. In dem Moment, wo der menschliche Geist durch die Technisierung erschlossen und damit die Technisation erreicht wird, wird nämlich die Bezeichnung „smart" plötzlich zu etwas, das auch wieder auf den Menschen zutrifft. Jedoch bleibt es weiterhin eine technische Spezifikation und der Mensch, der einst im Zentrum des IoT stand, könnte Teil der smarten Gerätelandschaft werden, deren Mittelpunkt dann nicht mehr der Nutzer ist, sondern nur noch die Daten: eine Metamorphose vom Homo Sapiens zum Smart Human.[30]

IV. Datenschutzrechtliche Fragen bei Smart Human

Diese Arbeit hat es sich zur Aufgabe gemacht, zu untersuchen, ob diese Metamorphose zum Smart Human durch bestehende datenschutzrechtliche Vorgaben sinnvoll begleitet werden kann. Dies bedeutet, dass überprüft werden soll, ob das derzeitige EU-Datenschutzrecht ausreichend ist, um

30 *Oettel,* DuD 2020, S. 386 (386 f.).

Neurotechnologie und die damit einhergehende neuartige Datenverarbeitung zu regulieren. Konkret bedeutet dies, dass betrachtet werden soll, ob mittels BCI überhaupt personenbezogene Daten verarbeitet werden und ob es sich um besondere Kategorien von personenbezogenen Daten handelt, welche Rechtsgrundlage herangezogene werden kann, wie das Auskunftsrecht bei dieser Technologie gewährleistet werden sollte, wie der technische Datenschutz aussehen könnte, ob Datenschutz-Folgenabschätzungen notwendig sein dürften, wie diese aussehen könnten und wie die Datenschutz-Grundsätze umgesetzt werden könnten.

Um diese Fragen beantworten zu können, soll einleitend dargelegt werden, was BCI überhaupt sind, wie diese funktionieren und warum bei dieser neuartigen Technologie Datenschutz so relevant ist. Darauf aufbauend sollen die maßgeblichen Artikel der Datenschutz-Grundverordnung (DGVO) analysiert werden, um die Ergebnisse dann auf BCI und deren Datenverarbeitung anzuwenden. Damit soll eingeschätzt werden, ob die bisherigen Reglungen bereits ausreichend sind. Die daraus resultierenden Erkenntnisse sollen dann genutzt werden, um Vorschläge zu präsentieren, wie die DSGVO angepasst werden könnte, um in Zukunft Nutzer von BCI besser datenschutzrechtlich zu schützen. Abschließend wird dann ein Fazit präsentiert, welches die Forschungsfragen nochmal aufgreift und beantwortet und einen kurzen Ausblick gibt.

B. Brain-Computer Interfaces (BCI)

I. Die Schnittstelle zum menschlichen Gehirn

Bereits 1875 wurde die Entdeckung gemacht, dass das Gehirn von Säugetieren elektrische Signale produziert.[31] Darauf aufbauend wurde ab 1929 die sog. EEG als grundlegendes Mittel der Hirnforschung entwickelt, womit die elektrischen Signale des Gehirns durch die Kopfhaut hindurch aufgezeichnet werden können.[32] Mit dieser Erfindung war ein historischer Durchbruch gelungen, der sowohl die Erforschung des menschlichen Gehirns, als auch die neurologische und psychiatrische Diagnostik bis heute bestimmt.[33]

1965 komponierte Musiker *Alvin Lucier* sein Stück „Music for Solo Preformer", welches mithilfe von Echtzeit-EEG gespielt werden musste, bei der Alpha-Wellen im Gehirn so weit verstärkt wurden, dass diese Schwingungen in Lautsprechern auslösten, welche wiederum Schlaginstrumente stimulierten.[34] Damit war eine der ersten grundlegenden Verknüpfungen des menschlichen Gehirns mit einer Maschine gelungen. Beinahe zeitgleich wurde die Methode des Neurofeedbacks entwickelt, mithilfe dessen die Selbstregulierung von Gehirnfunktionen erlernt werden sollte, indem Gehirnaktivität in Echtzeit analysiert, aufbereitet und dem Probanden als Rückmeldung dargestellt werden.[35] All diese Schritte führten letztendlich zur Erforschung der Möglichkeit von Gehirn Computer Kommunikation und zur Geburt der BCI.[36] Ebenso wurde damit die Technisierung des menschlichen Geistes eingeläutet.

---

31 *Caton,* British Medical Journal 1875, S. 278 (278).

32 *Berger,* Archiv für Psychiatrie und Nervenkrankheiten 1229, S. 527-570.

33 *Tudour/Tudor/Tudor,* Acta medica Croatica 2005, S. 307 (312 f.); *Millet,* Perspectives in Biology and Medicine 2001, S. 522 (540 f.).

34 *Straebel/Thoben,* Organised Sound 2014, S. 17 (22).

35 *Kamiya,* in: Charles Tart (Hrsg.), Altered States of Consciousness: A Book of Readings, 1969, S. 489 (489 ff.); bzgl. klinischer Anwendungsmöglichkeiten von Neurofeedback: *Sterman/Friar,* Electroencephalography and Clincal Neurophysiology 1972, S. 89 (92).

36 *Vidal,* Annual Review of Biophysics and Bioengineering 1973, S. 157 (157 ff.).

II. Funktion von BCI

Für die technologische Schnittstelle zum menschlichen Gehirn gibt es viele verschiedene Bezeichnungen und auch entsprechend viele Definitionen.[37] Doch um diese Arbeit so umfassend wie möglich zu gestalten, soll eine sehr inklusive und allgemeine Definition verwendet werden, die alle möglichen Ausgestaltungen berücksichtigt: BCI sind eine Verknüpfung des menschlichen zentralen Nervensystems, insb. des Gehirns, mit einem elektronischen System, wie bspw. einem Computer.[38]

Das zentrale Nervensystem ist dafür da, um äußere und innere Vorgänge, Einflüsse und Sinnesreize zu verarbeiten und entsprechende hormonelle oder neuromuskuläre Outputs zu generieren.[39] Diese Outputs sind das Resultat eines komplexen neuronalen und muskulären Zusammenspiels: Reize oder innere Vorgänge aktivieren bestimmte Hirnareale, die dafür sorgen, dass entsprechende Signale durch das Nervensystem geschickt werden, welches wiederrum die jeweiligen Muskeln ansteuert, um die gewollte Aktion bzw. Reaktion auszuführen.[40] Um dies zu bewerkstelligen, sind verschiedene elektrophysiologische, neurochemische und metabolische Prozesse verantwortlich, die sich bspw. als elektrische oder magnetische Signale im Gehirn bemerkbar machen.[41] Genau diese Signale können BCI aufzeichnen und in Outputs umwandeln.[42] Diese Output-Generierung kann entweder durch exogene oder endogene Reize/Signale veranlasst werden.[43] Eine Veranlassung durch exogene Reize liegt vor, wenn visuelle oder auditive Stimuli eine Aktion/Reaktion hervorrufen, wohingegen eine Veranlassung durch endogene Signale eintritt, wenn unabhängig von physikalisch manifestierten Stimuli, allein durch die Kontrolle der eigenen Gehirnaktivitäten, ein Output erzeugt wird.[44] Um aus exogen oder endogen erzeugten Hirnak-

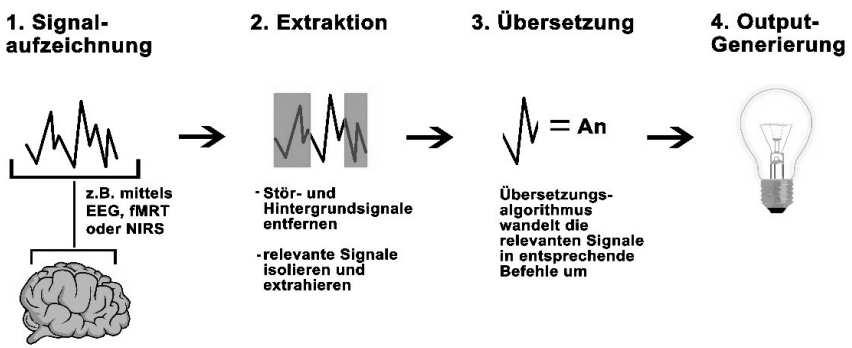
37 *Clément,* Brain-Computer Interface Technologies, 2019, S. 1.
38 *Guger et al.,* in: Guger, Brain-Computer Interface Research, 2024, S. 1 (1); *Peksa/Mamchur,* Sensors 2023, S. 1 (1); *Clément,* Brain-Computer Interface Technologies, 2019, S. 1.
39 *Liyanage/Bhatt,* in: Dey/Shour/Fong, Wearable and Implantable Medical Devices, 2020, S. 55 (56); *Wolpaw/Winter Wolpaw,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 3 (3).
40 *Baek et al.,* Computational Intelligence and Neuroscience 2019, S. 1 (1).
41 *Wolpaw/Winter Wolpaw,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 3 (4).
42 *Guger et al.*, in: Guger et al., Brain-Computer Interface Research, 2019, S. 1 (1).
43 *Orban et al.,* Bioengineering 2022, S. 1 (6 f.).
44 *Mugdal et al.,* Interdisciplinary Neurosurgery 2020, S. 1 (2).

tivitäten entsprechende Outputs zu generieren, gibt es für ein BCI zwei Möglichkeiten:[45]

1) Goal selection: Hier teilt der Nutzer dem BCI lediglich das Ziel mit, welches erreicht werden soll. Bspw. teilt der Nutzer per Gedanke mit, dass er mit seinem automatisierten Rollstuhl in die Küche möchte. Das BCI übermittelt diese Zielvorgabe an die Software des automatisierten Rollstuhls, welche dann den gesamten Prozess autonom steuert, bis der Nutzer in der Küche angekommen ist.
2) Process control: Hier ist der Nutzer in alle Details des Prozesses involviert und steuert den automatisierten Rollstuhl zu jeder Zeit. Der automatisierte Rollstuhl erreicht das Ziel somit nicht mehr auf seine eigene Art und Weise, sondern führt lediglich alle Befehle des Nutzers aus.

Bei beiden Möglichkeiten folgen BCI zusammengefasst vier Schritten: 1. Signalaufzeichnung, 2. Extraktion von relevanten Signalen, 3. Übersetzung der relevanten Signale und 4. Output-Generierung.[46]

Abbildung 1: Funktionsweise BCI.



Zu Beginn werden bei der Signalaufzeichnung die Gehirnaktivitäten mithilfe von Sensoren aufgezeichnet. Dafür können verschiedene Technologien eingesetzt werden, die in Kapitel C.I.I.a und b. genauer thematisiert werden. Da bei der initialen Aufzeichnung der Gehirnaktivitäten auch weitere

45 *Wolpaw/Winter Wolpaw,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 3 (9 f.).

46 *Maiseli et al.,* Brain Informatics 2023, S. 1 (2); *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (270); *Peksa/Mamchur,* Sensors 2023, S. 1 (2).

irrelevante Stör- und Hintergrundsignale aufgezeichnet werden, müssen fortführend die für die Handlung relevanten Signale isoliert und extrahiert werden.[47] Dies wird automatisiert durch eine Signalverarbeitungs-Software vorgenommen.[48] Erst danach kann mithilfe eines Übersetzungsalgorithmus, welcher sich bspw. Deep Learning oder Machine Learning Methoden bedient, eine Konvertierung der relevanten Signale zu entsprechenden Befehlen stattfinden.[49] Dieser Befehl wird abschließend an das externe Gerät weitergeleitet, welches dann den gewünschten Output erzeugt.[50] Um die Zusammenarbeit dieser einzelnen Schritte und die Interaktion mit dem Nutzer zu überwachen, bedarf es übergeordnet noch einer einheitlichen Betriebsumgebung, bei der alle Funktionen zusammenlaufen, koordiniert und kontrolliert werden.[51]

BCI ermöglichen dem Nutzer somit neue künstliche Formen von Outputs, die das natürliche komplexe Zusammenspiel zwischen Gehirn, Nervensystem und Muskeln umgehen,[52] somit nicht hormonell oder neuromuskulär sind und die herkömmlichen natürlichen Outputs entweder ersetzen, wiederherstellen, aufwerten, ergänzen oder verbessern können.[53] So kann bspw. die verlorene Fähigkeit des Gehens dadurch ersetzt werden, dass ein automatischer Rollstuhl per BCI gesteuert wird, die Funktion von gelähmten Armen durch BCI wiederhergestellt werden, die Aufmerksamkeit von Personen aufgewertet werden, indem BCI die Gehirnaktivität

47 *Krusienski/McFarland/Principe,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 123 (123); *Maiseli et al.,* Brain Informatics 2023, S. 1 (2); *Peksa/Mamchur,* Sensors 2023, S. 1 (2).

48 *Santamaría-Vázquez et al.,* Computer Methods and Programs in Biomedicine 2023, S. 1 (2); *Dong et al.,* Cyborg and Bionic Systems 2023, S. 1 (2); *Guger et al.*, in: Guger et al., Brain-Computer Interface Research, 2019, S. 1 (1); *Wilson/Guger/Schalk,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 165 (176 ff.).

49 *Hossain et al.,* Frontiers in Computational Neuroscience 2023, S. 1 (2); *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (272); *Santamaría-Vázquez et al.,* Computer Methods and Programs in Biomedicine 2023, S. 1 (2); detaillierter: *McFarland/Krusienski,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 147 (147 ff.); *Peksa/Mamchur,* Sensors 2023, S. 1 (11 ff.).

50 *Dong et al.,* Cyborg and Bionic Systems 2023, S. 1 (2); *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (272).

51 *Santamaría-Vázquez et al.,* Computer Methods and Programs in Biomedicine 2023, S. 1 (2); *Guger et al.*, in: Guger et al., Brain-Computer Interface Research, 2019, S. 1 (1).

52 *Baek et al.,* Computational Intelligence and Neuroscience 2019, S. 1 (1 f.); *Wolpaw/Winter Wolpaw,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 3 (6 ff.); *Mugdal et al.,* Interdisciplinary Neurosurgery 2020, S. 1 (2).

53 *Wolpaw/Winter Wolpaw,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 3 (3 f.).

überwacht und bei Aufmerksamkeitsverlust Alarm schlägt, die Handlungsfähigkeit ergänzt werden, indem z.B. ein zusätzlicher Roboterarm per BCI gesteuert werden kann und die eingeschränkte Möglichkeit, Gliedmaßen zu bewegen (bspw. aufgrund eines Schlaganfalls), durch BCI verbessert werden.[54]

1. Nicht-invasive BCI

Bei einem nicht-invasiven Einsatz von BCI können die Neurodaten durch externe Geräte aufgezeichnet werden. Diese Aufzeichnung ist mithilfe vieler verschiedener Methoden möglich. Weit verbreitet und gut erforscht ist der diesbezügliche Einsatz von EEG, bei der Elektroden direkt an der Kopfhaut angebracht werden.[55] EEG zeichnet sich durch eine einfache, portable Nutzung und niedrige Kosten aus, aber weist dafür oftmals eine gewisse Ungenauigkeit auf, da Signale nur global aufgezeichnet werden können.[56] Bessere und schnellere Ergebnisse liefert die Magnetenzephalographie (MEG) und die Magnetresonanztomographie (fMRT), sind dafür aber, aufgrund der Größe, der notwendigen Fixierung des Kopfes und dem magnetischen Feld, kaum flexibel einzusetzen.[57] Neben diesen beiden verbreiteten Methoden gibt es alternativ noch die relativ günstige und portable Möglichkeit der Nahinfrarotspektroskopie (NIRS), bei der anhand des Blutflusses Aktivitäten im Gehirn erkannt werden.[58]

Alle nicht-invasiven Methoden haben jedoch gemeinsam, dass sie für den Nutzer recht unkomfortabel sind, da es bei der EEG-Methode bspw. oftmals notwendig ist, die Haut kahl zu rasieren und ein Gel aufzutragen, welches die Signale besser leitet.[59] Allerdings werden die nicht-invasiven

54 Ebenda, S. 3 (4 f.).
55 *McFarland/Wolpaw,* Current Opinion in Biomedical Engineering 2017, S. 194 (198).
56 *Bansal/Mahajan,* EEG-Based Brain-Computer Interfaces: Cognitive Analysis and Control Applications, 2019, S. 63; *Zhang/Wang/Fuhlbrigge,* Proceedings of the 2010 IEEE 2010, S. 379 (380); *Zhao et al.,* Brain Sciences 2023, S. 1 (1 f.).
57 *Kosmyna/Lécuyer,* PLoS One 2019, S. 1 (4 f.); *Zhang/Wang/Fuhlbrigge,* Proceedings of the 2010 IEEE 2010, S. 379 (380); *Saha et al.,* Frontiers is Systems Neuroscience 2021, S. 1 (5).
58 *Zhang/Wang/Fuhlbrigge,* Proceedings of the 2010 IEEE 2010, S. 379 (378).
59 *Liyanage/Bhatt,* in: Dey/Shour/Fong, Wearable and Implantable Medical Devices, 2020, S. 55 (69 f.).

BCI kontinuierlich weiterentwickelt, sodass die Genauigkeit, Verlässlichkeit und der Tragekomfort zukünftig steigen dürften.[60]

2. Invasive/Semi-Invasive BCI

Invasive und semi-invasive BCI liefern die beste Signalqualität und aussagekräftige Ergebnisse.[61] Während bei der semi-invasiven Methode Elektroden unter der Kopfhaut direkt auf dem Schädel platziert werden, wird bei der invasiven Methode sogar die Schädeldecke geöffnet, um sehr feine Elektroden direkt auf oder in der Großhirnrinde zu implantieren.[62] *Elon Musks* Unternehmen Neuralink, das sich auf invasive BCI spezialisiert hat, möchte per Roboter 96 Fäden in die Großhirnrinde implementieren, die insg. 3.072 Elektroden beinhalten.[63] Anfang 2024 implantierte Neuralink tatsächlich ihren ersten Chip in einem Menschen.[64] Ein solcher chirurgischer Eingriff birgt allerdings Gefahren für den Nutzer. Es können Schäden am Hirngewebe, Infektionen und Nervenschäden auftreten sowie unvorhersehbare Reaktionen des Gewebes auf die Elektroden hervorgerufen werden.[65] Allerdings werden bereits neue Materialen und Modelle erforscht, die eine langfristige Verträglichkeit, Stabilität und Kompatibilität gewährleisten sollen.[66]

60 *Ferracuti et al.,* Brain Sciences 2022, S. 1 (10 f.); *Knierim/Bleichner/Reali,* Sensors 2023, S. 1 (2 ff.).

61 *Saha et al.,* Frontiers is Systems Neuroscience 2021, S. 1 (4); *Mak/Wolpaw,* IEEE Reviews in Biomedical Engineering 2009, S. 189 f; *Zhao et al.,* Brain Sciences 2023, S. 1 (2).

62 Clément, Brain-Computer Interface Technologies, 2019, S. 60 f.; *Kawala-Sterniuk,* Brain Sciences 2021, S. 1 (13); *Zhao et al.,* Brain Sciences 2023, S. 1 (2).

63 *Musk/Neuralink,* An Integrated Brain-Machine Interface Platform with Thousands of Channels, v. 16.7.2019, https://www.biorxiv.org/content/10.1101/703801v4.full.pdf (abgerufen 16.1.2021).

64 *Drew,* Elon Musk's Neuralink brain chip: what scientist think of first human trial, v. 2.2.2024, https://www.binasss.sa.cr/bibliotecas/bhm/feb24/34.pdf (abgerufen 7.4.2024).

65 *Salahuddin/Gao,* Frontiers in Neuroscience 2021, S. 1 (3 ff.); *Otto/Ludwig/Kipke,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 79 (92 ff.).

66 *Tang et al.,* nature electronics 2023, S. 109 (109 ff.); *Pampaloni et al.,* Frontiers in Neuroscience 2019, S. 1 (2 ff.).

III. Aktuelle Anwendungsmöglichkeiten

1. Medizinische Anwendungsmöglichkeiten

BCI werden derzeit hauptsächlich im medizinischen Bereich erforscht und verwendet, mit dem Ziel, erkrankten Menschen, die bspw. teilweise oder vollständig bewegungsunfähig sind, einen gewissen Grad an Selbstständigkeit zurückzugeben. Besonders bei Erkrankungen/Beschädigungen des motorischen Nervensystems (wie z.B. Amyotrophe Lateralsklerose, Zerebralparese oder Rückenmarksverletzungen) kommen BCI zum Einsatz, da diese die natürlichen, aber in diesen Fällen beschädigten, neuromuskulären Abläufe umgehen können.[67]

Die diesbezüglichen Anwendungsmöglichkeiten sind vielfältig. Gut erforscht ist die Kommunikation mithilfe von BCI für Personen, die vollständig paralysiert sind oder auf sonstige Art und Weise die Sprechfähigkeit verloren haben. Derartige Nutzer können mithilfe von Gehirnsignalen Buchstaben auswählen und Nachrichten schreiben oder sogar vom System synthetisiert aussprechen lassen.[68] Diese Methode kann auch genutzt werden, um durch das World Wide Web zu browsen.[69]

Neben Kommunikation können BCI beeinträchtigten Personen auch eine gewisse Autonomität ermöglichen. So kann bspw. ein automatisierter Rollstuhl per Gedanke gesteuert werden[70] sowie diverse Hilfsroboter.[71] Gelähmte Gliedmaßen können auch per BCI bewegt werden, bspw. mithilfe eines Exoskeletts oder durch auf der Haut angebrachte Elektroden, die die

67 *Peksa/Mamchur,* Sensors 2023, S. 1 (18 f.); *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (268); *Karikari/Koshechkin,* Biophysical Reviews 2023, S. 1 (1).

68 Einen guten Überblick bieten: *Rupp et al.,* in: Grübler/Hildt, Brain-Computer Interfaces in their ethical, social and cultural contexts, 2014, S. 7 (10); *Bansal/Mahajan,* EEG-Based Brain-Computer Interfaces: Cognitive Analysis and Control Applications, 2019, S. 58 ff.; Explizite Beispiele: *Birbaumer et al.,* Nature 1999, S. 297 (297 f.); *McCane et al.,* Clinical Neurophysiology 2015, S. 2124 (2124 ff.); *Nijboer et al.,* Clinical Neurophysiology 2008, S. 1909 (1909 ff.); *Shah et al.,* Sensors 2022, S. 1 (9 ff.).

69 *Mugler et al.,* IEEE Transactions on Neural Systems and Rehabilitation Engineering 2010, S. 599 (599 ff.); *Bensch et al.,* Computational Intelligence and Neuroscience 2007, S. 1 (1 ff.).

70 *Cao et al.,* Journal of Neuroscience Methods 2014, S. 33 (33 ff.); *Herweg et al.,* Biological Psychology 2016, S. 117 (117 ff.).

71 *Tonin et al.,* Proceedings of the annual international conference of the IEEE EMBS 2011, S. 1 (1 ff.); *Stawicki/Gembler/Volosyak,* Computational Intelligence and Neuroscience 2016, S. 1 (1 ff.); *Xu et al.,* Mathematics 2022, S. 1 (8 ff.).

entsprechenden Muskeln stimulieren.[72] Alternativ ist eine Steuerung von Prothesen[73] oder Roboterarmen[74] möglich.

Auch bei der Diagnose und Therapie von diversen psychischen Krankheiten können BCI eingesetzt werden. So können bspw. Epilepsie, Gehirntumore, Parkinson und Schlafstörungen anhand von Gehirnsignalen frühzeitig erkannt[75] und bspw. Aufmerksamkeitsdefizite (z.B. ADS und ADHS),[76] mentale Erschöpfung[77] und Auswirkungen von Schlaganfällen behandelt werden.[78] Bei der Wiederherstellung der Funktion der oberen Gliedmaßen bei Schlaganfallpatienten erzielen BCI mittlerweile sogar bessere Resultate als herkömmliche Therapien.[79]

2. Nicht-medizinische Anwendungsmöglichkeiten

Neben dem ausschließlich medizinischen Einsatz von BCI, entstehen auch immer mehr Anwendungsgebiete, die nicht ausschließlich medizinischer Natur sind oder sogar völlig davon losgelöst sind.[80] Ein aktuelles Forschungsfeld für nicht ausschließlich medizinische Anwendung von BCI ist die Steuerung eines Smart Homes per Gedanke, womit ein Anschluss des Gehirns an das IoT erreicht wird. Dabei sollen diverse Anwendungen und Geräte (bspw. Lampen, Heizungen, Sonnenschutz, TV) mithilfe einer entsprechenden Smart Home Software per BCI gesteuert werden können.[81]

---

72 *Soekadar et al.*, in: Guger et al., Brain-Computer Interface Research, 2019, S. 53 (53); *Bockbrader,* Current Opinion in Biomedical Engineering 2019, S. 85 (86).

73 *Yanagisawa et al.*, Annals of Neurology 2012, S. 353 (360).

74 *Bousseta et al.,* IRBM 2018, S. 129 (130 ff.); *Xu et al.,* Electronics 2020, S. 1 (3 ff.); *Sanna et al.,* Information 2020, S. 1 (4 ff.).

75 *Bansal/Mahajan,* EEG-Based Brain-Computer Interfaces: Cognitive Analysis and Control Applications, 2019, S. 61.

76 *Teo et al.,* Research in Autism Spectrum Disorders 2021, S. 1 (6 ff.); *Lim et al.,* Child and Adolescent Psychiatry and Mental Health 2023, S. 1 (5 ff.).

77 *Ramírez-Moreno et al.,* Enviromental Research and Public Health 2021, S. 1 (11 ff.).

78 *Mattia/Molinari,* in: Grübler/Hildt, Brain-Computer Interfaces in their ethical, social and cultural contexts, 2014, S. 49 (50 f); *Sebastián-Romagosa et al.,* Frontiers of Neuroscience 2020, S. 1 (5).

79 *Pichiorri et al.,* Annals of Neurology 2015, S. 851 (857 f.); einen guten Überblick über Rehabilitationsmöglichkeiten bietet: *Orban et al.,* Bioengineering 2022, S. 1 (11 ff.).

80 Einen guten ersten Überblick bietet: *Peksa/Mamchur,* Sensors 2023, S. 1 (19 ff.).

81 *Miralles et al.,* The Scientific World Journal 2015, S. 1 (3 ff.); *Kosmyna et al.,* Frontiers in Human Neuroscience 2016, S. 1 (1 ff.); *Srijony et al.,* Proceedings of International Joint Conference on Advances in Computational Intelligence 2021, S. 1 (1 ff.).

Daneben können auch digitale Avatare[82] kontrolliert und Spiele per Gedanke gespielt werden.[83] So gibt es z.B. ein simples Fußballspiel, bei dem man durch die Vorstellung einer Handbewegung nach links oder rechts Tore schießen kann und das entweder zusammen (durch aufeinander abgestimmte Gehirnaktivitäten) oder gegeneinander gespielt wird.[84] Ebenso können mithilfe von BCI unter anderem virtuelle Helikopter geflogen[85] sowie bspw. Pacman,[86] Pinball,[87] Tetris,[88] World of Warcraft[89] und noch etliche weitere Spiele[90] gespielt werden. Ein Einsatz in Virtual Reality- und Augmented Reality-Umgebungen wird im Zuge dessen auch bereits untersucht und erprobt.[91]

Auch in vielen Bereich der bildenden Kunst können BCI-Anwendung finden. So ist es z.B. möglich mit Hirnströmen Bilder zu malen[92] und sogar ganze Kunstinstallationen zu steuern.[93] Ebenso können per BCI-Instrumente gespielt werden.[94] Auch im Bereich FashionTech haben BCI bereits Einzug gehalten, sodass Kleidungsstücke auf Gedanken und psychischen Zustand reagieren können.[95]

---

82 *Guger/Allison*/Edlinger, in: Grübler/Hildt, Brain-Computer Interfaces in their ethical, social and cultural contexts, 2014, S. 85 (91).

83 *Paszkiel et al.,* NeuroSci 2021, S. 109 (112 ff.); *Peksa/Mamchur,* Sensors 2023, S. 1 (19 f.).

84 *Bonnet/Lotte/Lécuyer,* IEEE Transactions on Computational Intelligence and AI in Games 2013, S. 185 (185 ff.).

85 *Royer et al.,* IEEE Transactions on Neural Systems and Rehabilitation Engineering 2010, S. 581 (581 ff.).

86 *Reuderink/Nijholt/Poel,* in: Nijholt/Reidsma/Hondorp, Intelligent Technologies for Interactive Entertainment, 2009, S. 221 (221 ff.).

87 *Tangermann et al.,* Advances in Neural Information Processing Systems 2008, S. 1641 (1641 ff.).

88 *Pires et al.,* Proceedings of the 2013 IEEE 2nd International Conference on Serious Games and Applications for Health 2011, S. 1 (1 ff.).

89 *van de Laar et al.,* IEEE Transactions on Computational Intelligence and AI in Games 2013, S. 176 (177 ff.).

90 *Moore Jackson/Mappus,* in: Tan/Nijholt, Brain Computer Interfaces Applying our Minds to Human-Computer Interaction, 2010, S. 89 (S. 95 f.).

91 *Kohli et al.,* Microprocessors and Microsystems 2022, S. 1 (5 ff.).

92 *Müßinger et al.,* Frontiers in Neuroscience 2010, S. 1 (2 ff.).

93 *Jade/Gentle,* in: Nijholt, Brain Art, 2019, S. 229 (232 ff.).

94 *Reck Miranda et al.,* Proceedings of International Computer Music Conference 2005, S. 1 (1 ff.).

95 *Cass*, The Tech Behind the Mind-Reading Pangolin Dress Could Lead to Wireless - and Batteryless - Exoskeleton Control, v. 11.9.2020, https://spectrum.ieee.org/the-tech-behind-a-mind-reading-dress-could-lead-to-wireless-batteryless-exoskeleton-control (abgerufen 06.1.2025).

Des Weiteren können BCI als Sicherheits- und Authentifizierungsmechanismen fungieren.[96] Dabei werden spezifischen Signale aus dem Gehirn genutzt, um bspw. die Identität einer Person zu bestätigen oder Zugang zu Informationen zu erhalten.[97] Da diese Signale sehr fälschungssicher sind und kaum kopiert oder gestohlen werden können, stellt diese Methode eine sicherere Alternative zu sonstigen derzeit gängigen Sicherheits- und Authentifizierungssystemen dar.[98]

Besonderes Aufsehen erregen die sog. Brain-to-Brain Interfaces. Dabei werden zwei unterschiedliche Gehirne mithilfe von BCI miteinander verknüpft, sodass nicht nur Informationen aus der Gehirnaktivität gelesen, sondern auch Informationen zurück ins Gehirn gesendet werden können.[99] Dies ermöglicht es mehreren Menschen gemeinsam per Gedanken Probleme zu lösen, indem sie bspw. kooperativ eine Art Tetris spielen, bei dem der ausführende Spieler nur aufgrund der Gehirnaktivitäten der anderen Mitspieler einen Spielstein rotiert oder nicht.[100] So kann durch Brain-to-Brain Interfacing per Gedanke der Körper eines anderen Menschen gesteuert werden, indem kognitive Befehle einer Person bei der jeweils anderen Person als aktive Handlungen umgesetzt wird.[101]

Abschließend ist noch anzumerken, dass nicht alle nicht-medizinischen Anwendungsmöglichkeiten einen direkten Vorteil für den Nutzer haben. Es gibt auch jene BCI, die lediglich die Hirnströme auswerten, um die Ergebnisse für Effizienz-/Effektivitätssteigerung und für Marketingzwecke zu nutzen.[102] Besonderes Interesse besteht darin, das menschliche Gehirn in Relation zur Arbeit und zu täglichen Situation zu untersuchen, um bspw. die Auswirkung von hoher Arbeitsbelastung und Ermüdung auf den Arbeitnehmer und auf den Arbeitsprozess als solchen zu analysieren.[103] Es wird also der kognitive Zustand einer Person überwacht, mit dem

96 *Landau/Puzis/Nissim,* AMC Computing Surveys 2020, S. 1 (12 ff.); *Qui et al.,* ACM Computing Surveys 2019, S. 1 (3 ff.).
97 *Abdulkader/Atia/Mostafa,* Egyptian Informatics Journal 2015, S. 213 (218).
98 Ebenda.
99 *Rao et al.*, PLOS ONE 2014, S. 1 (1).
100 *Jiang et al.*, Scientific Reports 2019, S. 1 (2 ff.).
101 *Rao et al.*, PLOS ONE 2014, S. 1 (3 ff.).
102 *Bansal/Mahajan,* EEG-Based Brain-Computer Interfaces: Cognitive Analysis and Control Applications, 2019, S. 62 f.
103 *Ramírez-Moreno et al.,* Enviromental Research and Public Health 2021, S. 1 (11 ff.); *Mehta/Parasuraman,* Frontiers in Human Neuroscience 2013, S. 1 (8).

Ziel der Effizienzsteigerung.[104] Im schulischen Kontext kann das gleiche Vorgehen genutzt werden, um Aufmerksamkeit zu messen und zu verbessern.[105] Im Bereich Neuromarketing werden die Hirnströme analysiert, um die Wirksamkeit von Marketingmaßnahmen bestimmen zu können, mit dem Zweck, diese noch besser auf den Menschen anzupassen.[106] Diese Methoden werden bereits in großen Unternehmen wie Disney oder Google eingesetzt.[107] Eine ähnliche Auswertung der Gehirnaktivitäten ist auch bei Reden oder Auftritten von Politikern ö.ä. Interessenvertretern möglich, wodurch relativ genau abgelesen werden kann, wer bspw. den entsprechenden Politiker (nicht) unterstützt.[108] Ebenso ist es möglich, anhand von Gehirnaktivitäten zu bestimmen, welche politische Ausrichtung eine Person hat.[109]

3. Ausblick und zukünftige Anwendungsmöglichkeiten

BCI sind noch lange nicht im Mainstream angekommen, geschweige denn im kollektiven Bewusstsein der Gesellschaft angelangt.[110] Die Bemühung, BCI für die breite Masse zugänglich zu machen, besteht aber,[111] sodass auch bereits etliche Unternehmen auf diese neuartige Technologie spezialisiert sind.[112] In Anbetracht der umfangreichen, bis dato schon existierenden Anwendungsmöglichkeiten, ist es sehr wahrscheinlich, dass der nicht-medizinische Markt in Zukunft von BCI erschlossen wird. Zieht man die Entwicklungen von anderen hoch disruptiven Technologien heran, wie z.B. des Personal Computers (PC) und des Smart Phones und deren Weg zur Massentauglichkeit, kann eine sehr grobe und grundlegende Schätzung gewagt werden, wie lange es dauert, bis sich BCI ggf. im Mainstream etabliert haben werden.

---

104 *Roy et al.,* 35th Annual International Conference of the IEEE EMBS 2013, S. 6607 (6607 ff.).
105 *Al-Nafjan/Aldayel,* Sustainability 2022, S. 1 (9 ff.).
106 *Nomura/Mitsukura,* Procedia Computer Science 2015, S. 131 (135 ff.).
107 *Ienca/Andorno,* Life Sciences, Society and Policy 2017, S. 1 (10 ff.).
108 *Vecchiato et al.,* 31st Annual International Conference of the IEEE EMBS 2009, S. 57 (59f.).
109 Zumindest im amerikanischen Zwei-Parteien System: *Schreiber et al.,* PLOS ONE 2013, S. 1 (2f.).
110 *Grübler/Hildt,* in: Grübler/Hildt, Brain-Computer Interfaces in their ethical, social and cultural contexts, 2014, S. 115 (116).
111 *Allison/Graimann/Gräser,* Intelligent Systems IEEE – Conference Paper 2008, S. 1 (4); *Zhang/Wang/Fuhlbrigge,* Proceedings of the 2010 IEEE 2010, S. 379 (381 ff.).
112 *Kawala-Sterniuk,* Brain Sciences 2021, S. 1 (14 ff.); *Sawangjai et al.,* IEEE Sensors Journal 2020, S. 3996 (3997 ff.).

Nach der Entwicklung des ersten funktionsfähigen Digitalrechners Z3 von Konrad Zuse im Jahre 1941,[113] dauerte es ca. 36 Jahre, bis mit dem Apple II 1977 der erste massentaugliche PC auf den Markt kam.[114] Bis wirklich eine vollständige Durchdringung der Gesellschaft durch PCs stattfand, vergingen noch weitere ca. 13 Jahre.[115] Der Grundstein für das heutige Smartphone wurde in den 1970ern gelegt, als die ersten Geräte konzeptioniert wurden, die Telefonie und Rechenleistung miteinander verbanden.[116] Allerdings dauerte es noch 47 Jahre, bis Apple 2007 das erste IPhone herausbrachte, womit Smartphones die bis dato bereits weitverbreiteten gewöhnlichen Mobiltelefone schlagartig ersetzten.[117] Folgt man diesen beiden Beispielen, dauert es ca. 50 Jahre, bis sich eine disruptive Technologie am Markt vollständig durchgesetzt hat. Die ersten theoretischen Schritte in Richtung BCI wurden bereits in den 1970ern gemacht, wobei aber in den 1990ern die tatsächlich ersten Studien an Menschen durchgeführt wurden,[118] die zu den derzeitigen BCI, wie sie hier in dieser Arbeit beschrieben sind, geführt haben. Somit würde eine wirkliche Massentauglichkeit von BCI rund um 2040 eintreten.

Es wird allgemein angenommen, dass BCI zuerst in der Gaming-Industrie adaptiert werden.[119] Die dort vorhandene Zielgruppe ist bereits daran gewöhnt Headsets o.Ä. zu tragen, hat großes Interesse an neuartiger Technologie und ist auch bereit, Geld für ergänzende Peripheriegeräte auszugeben.[120] Da es bereits etliche Entwicklungen auf dem Bereich BCI-Gaming gibt, ist ein weitreichendes Vordringen der Technologie in den Gaming-Bereich schon weit vor 2040 denkbar. Danach ist eine sukzessive Verbreitung in andere Bereiche wahrscheinlich. Nach der Gaming-Branche erscheint eine Adaption der Technologie in der Industrie naheliegend. Nach der um-

113 *Zuse,* in: Grötschel et al., Vision als Aufgabe – das Leibnitz Universum im 21. Jahrhundert, 2016, S. 111 (116 ff.).

114 *Abbate,* Proceedings of the IEEE 1999, S. 1695 (1696).

115 Durchdringung der Gesellschaft wird hier festgemacht an zwei Ereignissen: 1. Veröffentlichung des ersten wirklichen Betriebssystems Windows 3.0 im Jahre 1990, womit ein einfacherer Zugang zur neuen Technologie gewährleistet wurden und 2. die Erfindung von HTML 1989, womit der Grundstein für das World Wide Web gelegt wurde.

116 *Islam/Want,* PERVASIVE computing 2014, S. 89 (89).

117 Ebenda.

118 *Kawala-Sterniuk,* Brain Sciences 2021, S. 1 (14 ff.).

119 *van Erp/Lotte/Tangermann,* Computer 2012, S. 26 (28); *Liyanage/Bhatt,* in: Dey/Shour/Fong, Wearable and Implantable Medical Devices, 2020, S. 55 (70).

120 *Allison/Graimann/Gräser,* Intelligent Systems IEEE – Conference Paper 2008, S. 1 (4).

fangreichen Digitalisierung der Industrie unter der Bezeichnung „Industrie 4.0", könnte die „Industrie 5.0" die technische Hybridisierung der Arbeitnehmer beinhalten, um bspw. den mentalen und emotionalen Zustand von Personen zu überwachen, die schwere und risikoträchtige Maschinen bedienen oder die zeitgleiche und damit effizientere Steuerung von mehreren Maschinen zu ermöglichen. Rund um 2040 würden BCI dann in private Haushalte Einzug halten und alle Bereiche des privaten Lebens durchdringen.

Derzeit ist der Endverbrauchermarkt rundum BCI noch unbedeutend bzw. kaum kommerziell erfolgreich.[121] Damit eine Massentauglichkeit erreicht werden kann, bedarf es aber noch einige Weiterentwicklungen der bereits existierenden BCI. Diese müssen vor allem sicherer, zuverlässiger, nutzerfreundlicher (robuste, genaue und einfache Nutzung der Technologie/Software; ohne Gel und Rasur der Kopfhaut), langlebiger, kostengünstiger und auch ästhetischer werden, damit eine breite Adaption stattfinden kann.[122] Allerdings sind auf all diesen Gebieten bereits etliche Erfolge zu verzeichnen. So gibt es kabellose und universell einsetzbare BCI, die mit innovativen Deep-Learning Algorithmen und flexiblen Elektroden arbeiten[123] und individuelle anpassbare BCI, die kostengünstig mithilfe eines 3D-Druckers hergestellt werden können.[124]

Bei der Entwicklung von BCI lassen sich einige Trends ablesen, die zu ganz neuen Anwendungsmöglichkeiten führen bzw. die bestehenden Anwendungen weiter ausbauen werden. Derzeit erhalten bspw. passive BCI, die teilweise autonom arbeiten (z.B. um den mentalen und emotionalen Zustand zu überwachen) und nicht wie aktive und reaktive BCI zwangsläufig ein aktives Zutun der Nutzer benötigen, mehr Aufmerksamkeit.[125] Dies führt mit sich, dass BCI zukünftig vermehrt in der Bildung Anwendung finden könnten, indem die Konzentration und Aufmerksamkeit von Schü-

121 *Smalley,* Nature Biotechnology 2019, S. 978 (980 ff.); *Drew,* Nature Electronics 2023, S. 90 (91 ff.).

122 *Liyanage/Bhatt,* in: Dey/Shour/Fong, Wearable and Implantable Medical Devices, 2020, S. 55 (69 f.); *Smalley,* Nature Biotechnology 2019, S. 978 (980 ff.); *Hochberg/Anderson,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 317 (321).

123 *Mahmood et al.,* Nature Machine Intelligence 2019, S. 412 (413 f.).

124 *Auda et al.,* Adjunct Publication of the 33rd Annual ACM Symposium on UIST 2020, S. 70 (70 ff.).

125 *Kawala-Sterniuk,* Brain Sciences 2021, S. 1 (19).

lern und auch der Lernerfolg genau überwacht werden.[126] Daneben wird auch die Verbindung zwischen Menschen mithilfe von BCI derzeit intensiv erforscht. Hier wurde bereits ein System entwickelt, bei dem Gedanken in Berührungen übersetzt werden können, die dann mit weiterer unterstützender Technologie bei einer anderen Person tatsächlich fühlbar dargestellt werden.[127] Dies könnte in Zukunft dazu führen, dass auch Echtzeit-Kommunikation zwischen zwei Personen mit BCI abgebildet werden kann. Facebook arbeitet diesbezüglich an einem System, das Gedanken direkt in Textnachrichten übersetzt.[128]

Relevanter könnten in Zukunft auch die Fusion von BCI und anderen Technologien werden. Populär ist dabei die Verknüpfung mit Virtual und Augmented Reality[129] oder die Verknüpfung des menschlichen Gehirns mit KI.[130] Hier könnte als Ziel von BCI das transhumanistische Ideal der Erweiterung der menschlichen kognitiven Fähigkeiten gesehen werden.[131] Alle diese Entwicklungen führen auch zu einer umstrittenen Form von BCI, die hier abschließend noch genannt werden soll: militärische BCI. Es wird davon ausgegangen, dass BCI in den nächsten 20 bis 30 Jahren weitreichend bei militärischen Aktivitäten eingesetzt werden könnten.[132] Dies beinhaltet vor allem die Kommunikation von Kommandos, Strategien oder wichtigen Informationen, das Monitoring von Soldaten in Gefechtssituationen und ggf. die Anpassung vom emotionalen Zustand sowie die Verarbeitung von Schmerzen, das Upload von Wissen und auch die Steuerung von Kriegsmaschinen.[133]

126 *Wang/Jung,* PLOS ONE 2011, S. 1 (10); *van Erp/Lotte/Tangermann,* Computer 2012, S. 26 (30); *Al-Nafjan/Aldayel,* Sustainability 2022, S. 1 (9 ff.).

127 *Wang et al.,* IEEE International Conference on SMC 2020, S. 3488 (3489).

128 *Constine,* Facebook is building brain-computer interfaces for typing and skin-hearing, v. 19.4.2017, https://techcrunch.com/2017/04/19/facebook-brain-interface (abgerufen 6.1.2025).

129 *Gera,* The Neuroscience of Mind-Control Gaming, v. 26.11.2018, https://variety.com/2018/gaming/features/brain-computer-interface-neurable-1203036143/ (abgerufen 5.1.2025); *Kohli et al.,* Microprocessors and Microsystems 2022, S. 1 (5 ff.).

130 *Chudler/Johnson,* Brain-Computer Interfaces and the Future of Humanity, v. 23.4.2017, https://www.psychologytoday.com/us/blog/brain-bytes/201704/brain-computer-interfaces-and-the-future-humanity (abgerufen am 6.1.2025).

131 *Cinel/Valeriani/Poli,* Frontiers in Human Neuroscience 2019, S. 8 ff.

132 *Binnendijk/Marler/Bartels,* Brain-Computer Interfaces U.S. Military Applications and Implications, 2020, S. 17 ff.

133 Ebenda.

C. Big Data und dessen Gefahren

I. Big Data, Datenökonomie und Überwachung

Alle Geräte im IoT erheben ständig Daten. Das Fitnessarmband misst den Herzschlag, erhebt die gelaufenen Schritte und Kilometer, die smarte Steckdose zeichnet auf, wann wieviel Strom verbraucht wird, die smarten Glühbirnen, wann in welchem Raum das Licht an ist und das Smartphone fungiert als zentrale Steuerungseinheit, bei der alle Daten zusammenlaufen. Bei den enormen Datenmengen, die dabei entstehen, spricht man heutzutage von Big Data. Obwohl Big Data ein sehr unscharfer und nicht einheitlich definierter Begriff ist,[134] kann zusammenfassend behauptet werden, dass darunter enorme, heterogene und sich ständig wandelnde Datensätze zu verstehen sind, die nicht ohne sorgfältige Analyse oder sog. Data Mining[135] mithilfe neuer Technologien und Ressourcen verstanden und genutzt werden können.[136] Geschätzt lag die Größe der weltweiten Datensphäre 2018 bei ca. 33 Zettabytes, wobei davon ausgegangen wird, dass bis 2025 eine Menge von 175 Zettabytes erreicht wird.[137] Für Unternehmen ist Big Data und dessen Analyse insofern attraktiv, da Daten heutzutage einen hohen wirtschaftlichen Stellenwert einnehmen, auf deren Grundlage etliche Geschäftsmodelle basieren.[138] Hauptaugenmerk bei der Analyse ist die Optimierung der Unternehmensprozesse, besonders im Bereich Marketing, Kundenbindung und Service.[139] Dementsprechend werden die Datensätze vermehrt dazu genutzt, Prognosen wie z.B. über den Beziehungsstatus, den Gesundheitszustand, den Charakter, die Persönlichkeit und die Emotionen

134 *Chen/Mao/Liu*, Mobile Networks and Applications 2014, S. 171 (173).
135 *Gandy,* in: Haggerty/Ericson, The New Politics of Surveillance and Visibility, 2006, S. 363 (364); *Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (421).
136 *Rajaraman,* Resonance 2016, S. 695 (697); *Faaique,* International Journal of Mathematics, Statistics, and Computer Science 2024, S. 96 (99 f.).
137 *Reinsel/Gantz/Rydning,* The Digitization of the World, 2018, S. 3; Durch das gestiegene Datenaufkommen aufgrund der Corona Pandemie (mehr Streaming, Videokonferenzen, mehr Nutzung von Online-Diensten) werden die 175 Zettabytes bis 2025 jedoch wahrscheinlich bei Weitem übertroffen werden.
138 *Jöns,* Daten als Handelsware, 2016, S. 16.
139 *Ohlhorst,* Big Data Analytics, 2013, S. 11 f.

zu erstellen, um gezielte Werbung oder Services anbieten zu können.[140] Diese Analyseergebnisse und Prognosen, und nicht die Daten selbst, werden nicht nur für die Optimierung der eigenen Unternehmensprozesse und des eigenen Marketings genutzt,[141] sondern auch Dritten angeboten, wie z.B. im Falle von Googles personalisierter Werbung.[142] Im Gegensatz dazu besteht aber auch ein expliziter Handel mit Daten wie z.B. Adresshandel, Scoring oder Data Broking.[143] Das wirtschaftliche Interesse an Daten ist dementsprechend groß.

Allerdings hat Big Data nicht nur kommerzielle Vorteile. Es kann genauso gut genutzt werden, um gesamtgesellschaftliche und wissenschaftliche Ziele zu verfolgen. So könnte die Big Data Auswertung im Gesundheitssektor bspw. hilfreich in der Diagnostik sein.[144] Außerdem könnte mittels Big Data ein digitaler Zwilling der Erde erzeugt werden, um bspw. Umweltauswirkungen besser vorherzusagen.[145] In der Astronomie werden durch einige Projekte bereits 100-200 Petabytes an Daten jährlich erzeugt, die ausgewertet werden können, um weitere Erkenntnisse über das Universum zu erhalten.[146]

Jedoch ist das Sammeln von solchen enormen Datensätzen und deren Analyse ein ambivalenter und umstrittener Prozess, denn auf der einen Seiten ist zwar das wirtschaftliche,[147] gesellschaftliche[148] und wissenschaftliche[149] Wertschöpfungspotential von Big Data enorm, auf der anderen Seite kann der Missbrauch dieser Daten aber auch schwerwiegende Konsequenzen haben. Im Zuge der Datenökonomie werden Privatpersonen ständig überwacht, da deren Daten und Erfahrungen als kostenloser Rohstoff für

140 *Christl,* Kommerzielle digitale Überwachung im Alltag, 2014, S. 12-24.
141 *Acciarini et al.,* Technovation 2023, S. 1 (4 ff.); *Krishna et al.,* 2023 International Conference on Inventive Computation Technologies 2023, S 1073 (1073 ff.).
142 *Jöns,* Daten als Handelsware, 2016, S. 17.
143 *Christl,* Kommerzielle digitale Überwachung im Alltag, 2014, S. 51-64.
144 *Akindote,* World Journal of Advanced Research and Reviews 2023, S. 1293 (1295 ff.).
145 *Li et al.,* Nature Reviews Earth & Environment 2023, S. 319 (320 ff.).
146 *Faaique,* International Journal of Mathematics, Statistics, and Computer Science 2024, S. 96 (100 ff.).
147 *Spiekermann,* Aus Politik und Zeitgeschichte 2019, S. 16 (18); *Acciarini et al.,* Technovation 2023, S. 1 (4 ff.); *Krishna et al.,* 2023 International Conference on Inventive Computation Technologies 2023, S 1073 (1073 ff.).
148 *Bitkom,* Leitlinien für den Big-Data-Einsatz, 2015, S. 22 ff.; *Akindote,* World Journal of Advanced Research and Reviews 2023, S. 1293 (1295 ff.).
149 *Spindler,* Medizinrecht 2016, S. 691 (691); *Li et al.,* Nature Reviews Earth & Environment 2023, S. 319 (320 ff.); *Faaique,* International Journal of Mathematics, Statistics, and Computer Science 2024, S. 96 (100 ff.).

Internetkonzerne fungieren können.[150] Da der Zugang zu Big Data restriktiv nur für einige wenige gewährleistet ist, wird Forschung verzerrt. Die großen Internetkonzerne, die in diesem Punkt als Gatekeeper bezeichnet werden können, können nach eigenem Ermessen entscheiden, wer Zugang zu den Datensätzen bekommt, zu welchem Zweck dies geschieht und so gezielt Einfluss auf die Forschung nehmen.[151]

Die größten Bedenken gegenüber Big Data gelten jedoch der Privatsphäre der betroffenen Personen und damit einhergehend auch deren Selbstbestimmung und Handlungsfreiheit. Denn mit der Verknüpfung und fortlaufenden Analyse von mehr und mehr Daten, hat alles plötzlich einen Personenbezug.[152] Jedes noch so unscheinbare Datum liefert neue Erkenntnisse über eine Person, da es mit bereits bestehenden Daten in Bezug gesetzt und entsprechend ausgewertet wird.[153] Auf staatlicher Ebene kann diese Dauerüberwachung von Einwohnern und die Erstellung detaillierter Profile auch als moderner Kontrollmechanismus ganz im Sinne des Orwellschen Big Brothers gesehen werden.[154] Dieser staatliche Kontrollmechanismus findet derzeit in Chinas Social Credit System seinen Höhepunkt. Dort werden gesellschaftsübergreifend auf Basis jeder sozialen und ökonomischen Tätigkeit der Einwohner Punkte verteilt, anhand derer entschieden wird, ob die jeweilige Person eine Belohnung oder eine Bestrafung für ihr Handeln erhält.[155] Die möglichen Implikationen eines solchen Systems, wie z.B. flächendeckende Zensur und Massenmanipulation, stellen eine ernstzunehmende Bedrohung der demokratischen Gesellschaft dar. Diese unterschwellige Beschneidung der individuellen Selbstbestimmung lässt sich jedoch auch in gewissen Zügen in Europa und den USA beobachten. In diesem Fall spielt Microtargeting, also das personen- und interessenspezifische Schalten von Inhalten,[156] eine große Rolle. Genau dieses Microtargeting wird vermehrt in der Konzeption von politischen Wahlkampagnen genutzt, indem anhand von Wahlprognosen und Scores, individuelle, auf Gruppen und Einzelpersonen zugeschnittene Maßnahmen entwickelt wer-

150 *Zuboff,* Aus Politik und Zeitgeschichte 2019, S. 4 (8).
151 *boyd/Crawford,* Information, Communication & Society 2012, S. 662 (675).
152 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1596 f. und 1599); *Frenzel* (2021), Art. 9 Rn. 8*; Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (422).
153 *Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (422).
154 *Bogard,* in: Haggerty/Ericson, The New Politics of Surveillance and Visibility, 2006, S.55 (59).
155 *Liang et al.,* Policy & Internet 2018, S. 415 (416).
156 *Zuiderveen Borgesius et al.,* Utrecht Law Review 2018, S. 82 (82).

den, welche die Stimmenvergabe bei Wahlen beeinflussen sollen.[157] Der wohl prominenteste Fall hierbei ist die Einflussnahme von Facebook und Cambridge Analytica auf die Präsidentschaftswahl 2016 in den USA.[158]

II. Bedeutung von Datenschutz

Big Data ist in der heutigen Gesellschaft ein Fakt und die Entwicklung lässt sich nicht mehr rückgängig machen. Die sinnvolle Gestaltung des Umgangs mit diesen Daten bleibt jedoch eine weitreichende rechtliche, ethische und technische Frage,[159] die es zu beantworten gilt.[160] Besonders die Bevölkerung sehnt sich nach einem effektiven Datenschutz, da diese vermehrt das Gefühl hat, Opfer von Datenklau und Datenmissbrauch zu sein[161] und sich wünscht, dass gerade sensible personenbezogene Daten, wie z.B. Gesundheitsdaten, vor Missbrauch geschützt werden.[162] Dementsprechend ist es nur 3 % der deutschen Internetnutzer egal, was mit ihren Daten passiert.[163] 42 % sind besorgt über die Menge an Daten, die Unternehmen über sie sammeln.[164] Ca. 26 % halten das Internet für wenig sicher – unsicher, wenn es um ihre personenbezogenen Daten geht.[165] Im Bereich Smart Home ist mangelnder Datenschutz bspw. ein Kriterium für die Nicht-Nutzung der Technologien.[166]

Auf der anderen Seite besteht jedoch auch das sog. Privacy Paradoxon, bei dem der Schutz von personenbezogenen Daten und der Privatsphäre

157 *Christl,* Aus Politik und Zeitgeschichte 2019, S. 42 (46 ff.).
158 *Chester/Montgomery,* Internet Policy Review 2017, S. 1 (7).
159 *boyd/Crawford,* Information, Communication & Society 2012, S. 662 (671 f.); *Boehme-Neßler,* International Data Privacy Law 2016, S. 222 (224); *Kasera et al.,* 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) 2023, S. 1122 (1122 ff.); *Vasa/Thakkar,* Journal of Computer Information Systems 2023, S. 608 (608 ff.).
160 *Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (423).
161 *Opaschowski,* in: Bäumler/von Mutius, Datenschutz als Wettbewerbsvorteil, 2002, S. 13 (14 ff.).
162 *Richter/Kliner/Rennert,* in: Knieps/Pfaff, Digitale Arbeit – Digitale Gesundheit, 2017, S. 107 (121).
163 *Bitkom,* Datenschutz in der digitalen Welt, 2015, S. 2.
164 Abrufbar unter: https://de.statista.com/statistik/daten/studie/1286512/umfrage/meinungen-der-deutschen-zum-thema-datenschutz-nach-generationen/ (abgerufen 7.4.2024).
165 Abrufbar unter: https://www.sicher-im-netz.de/file/14331/download?token=i7DCJrK4 (abgerufen 7.4.2024).
166 *Deloitte*, Smart Home Consumer Survey 2018, 2018, S. 15.

zwar als wichtig eingestuft wird, aber nicht zwangsläufig das Verhalten der Nutzer bestimmt.[167] Dabei findet eine einfache Kosten-Nutzen-Abwägung statt, bei der die erhaltene Leistung, die auf Preisgabe von Daten basiert, als größerer Vorteil eingestuft wird, als der Erhalt der Privatsphäre.[168] Erklärungen für dieses Phänomen gibt es viele,[169] hier soll jedoch zusätzlich argumentiert werden, dass eine Korrelation zwischen der Angst, etwas zu verpassen,[170] und dem Mangel an datenschutzfreundlichen und vergleichbaren Alternativen zu den etablierten Anbietern besteht. Um nicht vom gegenwärtigen gesellschaftlichen Leben ausgeschlossen zu werden, hat sich die Nutzung von Social Media, Smartphones, Apps etc. zu einem essenziellen Bestandteil der Moderne entwickelt, der nur durch die Beschränkung der Privatsphäre erhalten werden kann. 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.[171] Diese Unsicherheit gepaart mit dem Privacy Paradoxon kommt dann oftmals Internetunternehmen zugute.[172]

167 *Engels,* IW-Trends 2018, S. 3 (6).
168 *Engels/Grunewald,* IW-Kurzberichte 2017 (57), S. 1 (1).
169 *Barth/de Jong,* Telematics and Informatics 2017, S. 1038 (1038 ff.).
170 *Przybylski et al.,* Computer in Human Behavior 2013, S. 1841 (1842).
171 *Bitkom,* Datenschutz in der digitalen Welt, 2015, S. 3.
172 *Engels,* IW-Trends 2018, S. 3 (6).

D. BCI und Datenschutz

I. BCI als Herausforderung für den Datenschutz

Wie unter Kapitel B.III.1-3 beschrieben, können mithilfe von BCI bspw. diverse Gesundheitszustände festgestellt, Befehle identifiziert und Zustimmung oder Ablehnung erkannt werden. Gehirnströme/Gehirnaktivitäten als solche bieten aber noch ein viel weitreichenderes Informationsschöpfungspotential. Es können bspw. konkrete Wörter aus Neurodaten ausgelesen[173] und Inhalte von Sätzen vorhergesagt werden.[174] Dies gilt nicht nur für Sätze, sondern teilweise auch schon für Intentionen bezüglich zukünftiger Handlungen.[175] Ebenso können Gesichter, die der Nutzer sieht, anhand von Gehirnaktivitäten mit hoher Übereinstimmung nachmodelliert werden.[176] Dies ist grundlegend auch schon bei anderen visuellen Erfahrungen möglich, wie z.B. bei gesehenen Filmausschnitten o.Ä..[177] Damit könnten rein theoretisch alle visuellen Reize aus Neurodaten ausgelesen werden. Dies geht so weit, dass gesehene Gesichter auch später noch rudimentär aus dem Gedächtnis der Nutzer auslesbar sind.[178] Auf Grundlage von Neurodaten können ebenso Aussagen darüber getroffen werden, welche sexuelle Orientierung die betroffene Person hat,[179] ob es sich um einen Omnivoren, Vegetarier oder Veganer handelt,[180] ob jemand Alkoholiker oder Nicht-Alkoholiker ist,[181] ob jemand Raucher oder Ex-Raucher ist,[182] wie sexuell aktiv die Person ist,[183] ob die Person unter einer Essstörung leidet,[184] welcher Ethnie die Person zugehört,[185] und ob die Person stereotype Vorurteile gegenüber

173 *Moses et al.,* Nature Communications 2019, S. 1 (2 f.).
174 *Wang/Cherkassky/Just,* Human Brain Mapping 2017, S. 4865 (4874 ff.).
175 *Haynes et al.,* Current Biology 2007, S. 323 (323 ff.).
176 *Nemrodov et al.,* eNeuro 2018, S. 1 (4 ff.).
177 *Nishimoto et al.,* Current Biology 2011, S. 1641 (1641 ff.).
178 *Lee/Kuhl,* The Journal of Neuroscience 2016, S. 6069 (6075 ff.).
179 *Safron et al.,* Scientific Reports 2018 (8), S. 1 (7 ff.).
180 *Filippi et al.,* PLoS One 2010, S. 1 (2 f.).
181 *Vinothraj et al.,* Conference Papers IFSA-SCIS 2017, S. 1 (4 ff.).
182 *Nestor et al.,* Addiction Biology 2016, S. 369 (375 ff.).
183 *Hammilton/Meston,* Archive of Sexual Behavior 2017, S. 2289 (2294 f.).
184 *Groves/Kennett/Gillmeister,* Biology Psychology 2017, S. 205 (217 ff.).
185 *Tang et al.,* NeuroImage 2010, S. 33 (36 ff.).

anderen Geschlechtern und Ethnien hat.[186] Ebenso können diese Neurodaten Aussagen über die generellen kognitiven Fähigkeiten und Persönlichkeitszüge einer Person machen[187] und bestimmte neurokognitive Biomarker aufweisen, die bei entlassenen Gefängnisinsassen die Wahrscheinlichkeit der erneuten Straffälligkeit vorhersagen können.[188] Besonders kritisch ist die Tatsache, dass auch ohne Wissen der Nutzer persönliche Daten aus den Gehirnaktivitäten ausgelesen werden können. So ist es bspw. bereits möglich, mithilfe eines gängigen Gaming-BCI die Bankkarten-PIN, das dazugehörige Bankinstitut, den geographischen Standort, den Geburtsmonat und die Bekanntheit von Gesichtern/Personen zu ermitteln.[189] Dieses unbemerkte Auslesen von Informationen aus BCI-Daten wird auch als Brain Spyware bezeichnet und könnte in Zukunft zu Identitätsdiebstahl, Phishing und Betrug führen und dafür genutzt werden, um Passwörter zu entschlüsseln.[190] Generell besteht die Sorge, dass von sog. Brain Malware eine große Gefahr ausgehen könnte.[191] Aus diesem Grund bekommt die Sicherheit von BCI immer mehr Aufmerksamkeit.

Durch BCI werden zwangsläufig umfangreiche Neurodaten aufgezeichnet, die das Potential besitzen, weitreichende Informationen zu den Nutzern zu enthalten. Smart Human werden somit Datensätze generieren, die bis dato nie im großen Umfang verarbeitet wurden und der Datenökonomie eine weitere verwertbare Datenkategorie zur Verfügung stellen. Sie werden unter anderem die Kommerzialisierung der menschlichen Gedanken ermöglichen. In der Zukunft werden also auch Gedanken neben umfangreichen Nutzungsdaten, Standortdaten und Verhaltensdaten genutzt, um Prognosen wie z.B. über den Beziehungsstatus, den Gesundheitszustand, den Charakter, die Persönlichkeit und die Emotionen zu erstellen, damit gezielt Werbung geschaltet und Services angeboten werden können.[192] Dies wird derzeit bereits durch sog. Neuromarketing gewährleistet. Bedenkt man nun noch, dass die aufgezeichneten Gehirnaktivitäten auch dafür genutzt werden können, um bspw. die Zustimmung oder Abneigung

186 *Knutson et al.,* Human Brain Mapping 2007, S. 915 (927).
187 *Landau et al.,* Knowledge-Based Systems 2020, S. 1 (19 f.).
188 *Aharoni et al.,* PNAS 2012, S. 6223 (6224 ff.).
189 *Martinovic et al.,* Proceedings of the 21st USENIX Security Symposium 2012, S. 1 (5 ff.); Zur Identifikation von unterbewusster Gesichtserkennung: *Vargas Martin/Cho/Aversano,* ACM Transactions on Applied Perception 2016, Article 7 S. 1 (10 f.).
190 *Ienca/Haselager,* Ethics and Information Technology 2016, S. 117 (122).
191 *Bonaci/Calo/Chizeck,* IEEE Technology and Society Magazine 2015, S. 32 (36).
192 *Christl,* Kommerzielle digitale Überwachung im Alltag, 2014, S. 12-24.

zu Staatsoberhäuptern oder staatlichen Maßnahmen zu bestimmen, wird deutlich, dass BCI auch ein Instrument für großflächige staatliche Überwachung sein könnten. Allein aufgrund dieser beiden Tatsachen ist es geboten, Smart Human zukünftig umfangreich datenschutzrechtlich zu schützen.

II. Eine neue Art von Daten

1. Bedeutung von Daten

Um diesen umfangreichen datenschutzrechtlichen Schutz von Smart Human gewährleisten zu können, bedarf es einer initialen Auseinandersetzung mit dem Begriff „Daten" und dessen Bedeutung.

Das Konzept von Daten hat sich über die Menschheitsgeschichte langsam entwickelt und ausdifferenziert. Am Anfang dürften frühzeitliche Bedürfnisse nach Schutz und Sicherheit dazu geführt haben, dass Gegebenheiten in Zahlen dargestellt wurden (Anzahl an Bedrohungen, Länge eines Weges etc.).[193] Diese Vorgehensweise führte zur Verbreitung der Mathematik bis hin zum antiken pythagoreischen Verständnis, dass alles durch Zahlen beschrieben werden kann.[194] Darauf aufbauend erweiterte sich dann der Datenbegriff das erste Mal deutlich, als die moderne Wissenschaft entstand.[195] Daten wurden ab diesem Zeitpunkt als etwas verstanden, das Informationen erzeugen kann und somit dann ggf. zu Wissen führt.[196] Die Auseinandersetzung mit diesem Verständnis von Daten in der Wissenschaft, ist dabei ein ständig fortlaufender Prozess,[197] besonders seit der Entstehung von Big Data. Mit Big Data sind noch nie vorher dagewesene Datenmengen gemeint, die nur noch mittels neuer und besonderer Methoden ausgewertet werden können und die Vision nach einer umfänglichen Quantifizierbarkeit der Welt beflügeln.[198] Die Entwicklung hin zu Big Data hat auch dazu geführt, dass immer mehr Prozesse und Vorgänge datenge-

193 *Liu,* Procedia Computer Science 2014, S. 60 (61).
194 *Agrò*, Music and Astronomy, 2023, S. 16.
195 *Liu,* Procedia Computer Science 2014, S. 60 (62).
196 *Beck*, BIM im Facility Management, 2023, S. 36; *Liu,* Procedia Computer Science 2014, S. 60 (62).
197 *Olson*, Qualitative Health Research 2021, S. 1567 (1569).
198 *Liu,* Procedia Computer Science 2014, S. 60 (62 f.).

trieben und datenerzeugend sind, sodass nun quasi alles Informationen erzeugen kann - Daten sind also überall.[199]

Wenn Daten mittlerweile allgegenwärtig sind, stellt sich die grundlegende Frage, was Daten überhaupt sind. Im DUDEN werden Daten als „(durch Beobachtungen, Messungen u. a. gewonnene) [Zahlen]werte; (auf Beobachtungen, Messungen, statistischen Erhebungen u. a. beruhende) Angaben, Befunde; (persönliche) Kenngrößen, Merkmalsangaben" definiert.[200] Diese Definition dürfte allerdings nicht jeden zufriedenstellen. In der Informatik z.B. sind Daten nämlich nicht zwangsläufig Beobachtungen oder dergleichen, sondern vielmehr Repräsentationen von Informationen in einer vereinheitlichten Art und Weise.[201] Eine allgemein akzeptierte Definition von Daten gibt es demnach nicht.[202]

Der australische Philosoph *Brian Ballsun-Stanton* wagte allerdings einen umfassenden Definitionsversuch und arbeitete drei Kategorien zur Unterscheidung von Daten aus:[203]

1. Daten als Kommunikation: Daten sind Zeichen, die Botschaften und Nachrichten kodieren, unabhängig von der Darbietungsform und vom Realitätsbezug. Daten sind damit Aneinanderreihungen von Bits.
2. Daten als subjektive Beobachtungen: Daten sind subjektive Aussagen über die Realität, die kontextabhängig sind und Auswertung bedürfen, um Informationen zu erzeugen (z.B. Notizen, Aufzeichnungen, Interviews).
3. Daten als messbare Fakten: Daten sind objektive und wahre Aussagen über die Realität, die mittels Messungen erlangt wurden und welche reproduzierbar sind (z.B. Höhe eines Berges, Entfernung zum Mond).

Mit dieser Definition dürften verschiedene Verständnisse des Datenbegriffs gut miteinander vereinbar sein. Besonders, da verschiedene Kategorien auch gleichzeitig gelten können, womit der Anwendungsbereich nochmal erweitert wird. So sind bspw. Chat-Verläufe in Daten der Kategorie 1 und 2 einzuordnen oder physikalische Berechnungen in Daten der Kategorie 1 und 3. Lediglich Datenarten, die gleichzeitig der Kategorie 2 und 3 ent-

199 *Glaser*, The Grounded Theory Review 2007, S. 1 (1 ff.); *Liu,* Procedia Computer Science 2014, S. 60 (63).

200 Abrufbar unter: https://www.duden.de/rechtschreibung/Daten (abgerufen 2´7.4.2025).

201 Abrufbar unter https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v2:en (abgerufen am 27.4.2024); *Beck*, BIM im Facility Management, 2023, S. 35 f.

202 *Voß*, LIBREAS 2013, S. 1 (1).

203 *Ballsun-Stanton,* Asking About Data, 2012, S. 18 ff.

sprechen, können nicht vorliegen. Subjektive Beobachtungen können per Definition kaum gleichzeitig auch objektive Fakten sein und vice versa. Subjektiv bedeutet, dass es eben nicht objektiv ist. Es findet sprachlich eine klare Abgrenzung untereinander statt. Diese Abgrenzung ist auch sinnvoll und somit ist auch die entsprechende Aufteilung bei der Definition des Datenbegriffs nachvollziehbar. Demnach sollten keine Daten existieren, die sich gleichzeitig in alle Kategorien einordnen lassen. Allerdings könnten BCI auch hier, beim Verständnis des Datenbegriffs, ein wesentliches Umdenken anstoßen.

2. Neue Daten: Wesensdaten

In Kapitel D.I wurde bereits ausführlich dargelegt, dass es kaum möglich ist, dem Auswertungspotential von Neurodaten durch BCI Grenzen zu setzen. BCI können aufgrund von Neurodaten, die auch als neurologischen Rohdaten bezeichnet werden können, umfangreiche explizite Daten erzeugen. Diese erzeugten, expliziten Daten können keiner eindeutigen Datenkategorie zugeordnet werden, da je nach Beschaffenheit z.B. Gesundheitsdaten, Standortdaten, Bankdaten oder Wahrnehmungsdaten vorliegen könnten. Noch spezieller wird dieses Phänomen, wenn die eingangs präsentierte Definition von „Daten" angewandt wird. Neurodaten können ohne Probleme in die Kategorie 1 (Daten als Kommunikation) eingeordnet werden. Schließlich werden mittels BCI Hirnströme ausgelesen, übersetzt und übermittelt. Es findet somit eine Kodierung der neurologischen Signale in Bits statt. Auch in Kategorie 3 (Daten als messbare Fakten) lassen sich Neurodaten ohne Probleme einordnen. Mit BCI werden Hirnaktivitäten gemessen, um objektiv festzustellen, was tatsächlich neurologisch im menschlichen Gehirn vorgeht. Es werden damit objektive, wahre Aussagen über die Realität gemacht, da diese Signale tatsächlich existieren. Wie im vorherigen Kapitel beschrieben, sollte sich keine Datenart in mehr als zwei Kategorien einordnen lassen. Demnach dürften Neurodaten nicht auch noch unter Kategorie 2 (Daten als subjektive Beobachtungen) fallen. Allerdings werden mit BCI die Gehirne von Subjekten ausgelesen. In diesen Gehirnen wird die gesamte subjektive Wahrnehmung des Individuums verarbeitet - die Weltanschauung, die Zustimmung, die Ablehnung. Wenn also mittels BCI

gemessen wird, ob eine Person einem Politiker zustimmt oder nicht,[204] wird eine subjektive Aussage (Politiker XY ist gut/schlecht) erhoben. Neurodaten sind in ihrer Aussagekraft und der Ausgestaltungsmöglichkeiten somit so vielfältig, dass eine einzigartige Situation vorliegt: Rohdaten, die ohne weitere Maßnahmen nichts aussagen, aber durch Auswertung mit hoher Genauigkeit alles aussagen und darstellen können. Einen vergleichbaren Fall gibt es bis dato noch nicht.

Um dieser Sachlage gerecht zu werden und um eine Einordnung in die DSGVO vorzunehmen, ist es notwendig, eine terminologische Aufbereitung vorzunehmen, besonders da bestehende Bezeichnungen wie z.B. Neurodaten, Gehirnströme und Gehirnaktivitäten nicht umfassend genug sind.

Neurodaten zeichnen sich durch zwei Datensätze aus:[205] 1. Aufgezeichnete Gehirnaktivitäten/Gehirnströme, Neurodaten oder neurologische Rohdaten, die keine alleinige Aussagekraft haben und 2. Auswertung der neurologischen Rohdaten, die eine fallabhängige Aussagekraft besitzen. Hierbei wird nochmals deutlich, dass Neurodaten gleichzeitig objektive und subjektive Aussagen über die Realität machen. Die Rohdaten sind hier eine objektive Aussage über die Realität der Gehirnaktivitäten, während die Auswertung dieser Rohdaten subjektive Aussagen über die Wahrnehmung des Individuums sind.

Die fallabhängige Aussagekraft der Auswertung der Rohdaten kann weiterführend ebenso in zwei Kategorien unterteilt werden: 1. Aussagen über die äußeren Wesensmerkmale und 2. Aussagen über die inneren Wesensmerkmale. Äußere Wesensmerkmale sind Gegebenheiten, die sich direkt aus dem Erscheinungsbild oder aus dem Verhalten einer Person ergeben und z.B. Rückschlüsse auf Geschlecht, Ethnie oder Gesundheit zulassen. Hierunter fallen jene Auswertungen, die zwar mithilfe eines BCI gemacht werden können, aber nicht zwangsläufig eines BCI bedürfen, da auch auf anderem Wege zum selben Ergebnis gekommen werden kann. Innere Wesensmerkmale sind hingegen kognitive Prozesse, die Werte- und Moralvorstellungen entsprechen, Ansichten darstellen, Präferenzen kundtun, Orientierungen abbilden, Persönlichkeitszüge offenlegen und somit zusammenfassend als die Gedanken einer Person bezeichnet werden können. Im Gegensatz zu den äußeren Wesensmerkmalen sind diese inneren Wesens-

204 *Vecchiato et al.,* 31st Annual International Conference of the IEEE EMBS 2009, S. 57 (59f.).

205 *Latini,* To the edge of data protection: How brain information can push the boundaries of sensitivity, 2018, S. 22.

merkmale meist verborgen, nicht offensichtlich und können somit auch nur mithilfe eines BCI so umfassend ermittelt werden. Die Möglichkeit, detaillierte Aussagen über die inneren Wesensmerkmale zu machen, ist demnach ein Alleinstellungsmerkmal, das nur BCI vorenthalten ist.

Äußere und innere Wesensmerkmale einzeln betrachtet, können bereits ein detailliertes Bild einer Person zeichnen und weitreichende Auswertungen ermöglichen. Die wirkliche Sprengkraft liegt allerdings in der Kombination dieser beiden Dimensionen von Aussagen. Zusammen betrachtet entsteht eine ganzheitliche, präzise, intime und sezierende Darstellung einer Person und ihrer umfangreichen Facetten, die es in dieser Form noch nicht gegeben hat. BCI ermöglichen somit objektive Einblicke in das eigentliche subjektive Wesen der Nutzer. Das Wesen ist die Summe aller Eigenschaften und Merkmale einer Person, die ihr notwendigerweise zukommen müssen, um sie zu dieser einen spezifischen und vollkommen individuellen Person zu machen.[206] Smart Human werden damit eine neue Datenkategorie erschaffen: Wesensdaten.[207]

Um eine Einordnung von Wesensdaten in die DSGVO vorzunehmen, ist es notwendig, eine eindeutige Definition zu präsentieren. Wesensdaten liegen dann vor, wenn anhand eines neurologischen (Roh-)Datensatzes objektive Auswertungen vorgenommen werden können, die mithilfe von technologischer Erweiterung des menschlichen Gehirns und zentralen Nervensystems subjektive Outputs generieren können und/oder fallabhängige Aussagen über äußere und/oder innere Wesensmerkmale machen können, die eindeutige Rückschlüsse auf das individuelle Wesen einer Person zulassen.

206 *Aristoteles,* Die Kategorien, 2009, S. 13.

207 *Oettel,* DuD 2021, S. 632 (632 f.); kommen zu einem ähnlichen Ergebnis und schlagen die neue Datenart „kognitive biometrische Daten" vor, die allerdings nur auf die „mentalen Zustände" abstellt: *Magee/Ienca/Farahany,* Neuron 2024, S. 3017 (3022).

E. Die Notwendigkeit der datenschutzrechtlichen Regulierung

Folgt man der antiken rechtstheoretischen Annahme, die auch in der Moderne immer wieder aufgegriffen wird, ist Recht das normative Mittel, um Gerechtigkeit zu erreichen bzw. zu erhalten.[208] Gerechtigkeit ist dabei eine Eigenschaft, die in Relation zu anderen Wesen besteht[209] und objektiv die Verbindung zwischen Individuen mitsamt ihrer verschiedenen Zwecke, Willen und Bedürfnisse (rechtlich) reguliert.[210] Dabei sollte allerdings stets versucht werden, die Freiheit aller so weitrechend wie möglich zu erhalten.[211] Damit wird auch der Erhalt der individuellen und kollektiven Freiheit Teil der Gewährleistung von Gerechtigkeit und somit auch ein notwendiger Bestandteil des Rechts.[212]

Freiheit ist dabei eng an den freien Willen des Individuums geknüpft, wonach die Handlungsfreiheit, also die Möglichkeit einer Person, bewusst und freiwillig das zu tun, was sie will, ohne durch externe Hindernisse davon abgehalten zu werden,[213] besonders schützenswert ist. Diese wurde im deutschen Grundgesetz aufgegriffen und als allgemeine Handlungsfreiheit in Art. 2 Abs. 1 GG als umfassendes Auffanggrundrecht kodifiziert.[214] Ein wichtiger Baustein zur Gewährleistung von Handlungsfreiheit ist die Privatheit des Individuums.[215] Besonders eindrucksvoll wird dies bspw. durch die Beschränkung der Handlungsfreiheit in der DDR unterstrichen, die vor allem durch die umfassende Überwachung durch die Staatssicherheit entstand, da diese enorme Datensätze zum Großteil der Bevölkerung sammelte, um Systemfeinde zu identifizieren.[216] Freier Wille ist also nur

208 *Platon,* Der Staat, 2000, *S.* 97 ff; *Aristoteles,* Die Nikomachische Ethik, 1985, S. 101 ff.; *Radbruch,* Rechtsphilosophie, 2003, S. 34 ff.; *Rawls,* A Theory of Justice, 1971, S. 7 ff.

209 *von Aquin,* Summa Theologiae II-II, 1920, Frage 57, 1 und Frage 58, 2; *Platon,* Eutyphron, 2014, S. 39.

210 *Stammler,* Lehrbuch der Rechtsphilosophie, 1923, 197 ff.

211 *Rawls,* A Theory of Justice, 1971, S. 63 f.

212 *Fichte,* Grundlagen des Naturrechts und Principien der Wissenschaftslehre 1796, S. 10 ff; *Kant,* Die Metaphysik der Sitten, 2013, S. 24 f.

213 *Hobbes,* Leviathan, 1996, S. 107; *Boehme-Neßler,* International Data Privacy Law 2016, S. 222 (223 f.).

214 *Schmidt* (2021), Art. 2 Rn. 1 ff.

215 *Westin,* Privacy and Freedom, 1967, S. 23 ff; *Boehme-Neßler,* International Data Privacy Law 2016, S. 222 (223 f.).

216 *Gräßler,* War die DDR totalitär?, 2014, S. 140 ff.

dann möglich, wenn die Einzelperson sich gewiss sein kann, dass ihr aufgrund ihrer Gesinnung, Weltanschauung, Sexualität, Gedanken usw. keine Repressalien drohen. Und auch eine freie Entfaltung der Persönlichkeit ist nur möglich, wenn keine Sorge bestehen muss, welche Informationen gesammelt und verarbeitet werden.[217] Wie vorausgehend bereits dargelegt wurde, erzeugen BCI eine Menge solcher Daten, die Rückschlusse zu Personen in nie zuvor dagewesenem Umfang ermöglichen. BCI können das innerste Seelenleben der Menschen, ihre Gedanken, offenlegen. A priori lässt sich daraus schließen, dass personenbezogene Daten eine besondere Relevanz für die individuelle und allgemeine Handlungsfreiheit besitzen. Es besteht somit ein kausaler Zusammenhang zwischen Datenschutz und Handlungsfreiheit und demnach auch Freiheit als Ganzes. Aufgabe des Rechts ist es also, diese Kausalkette zu erkennen und zu berücksichtigen, da sie nur so tatsächlich das normative Mittel sein kann, um Gerechtigkeit zu erreichen bzw. zu erhalten. Ein umfangreicher Schutz von Smart Human ist demzufolge geboten.

Die Judikative in Deutschland und Europa hat diesen kausalen Zusammenhang zwischen Datenschutz, Freiheit und Gerechtigkeit bereits früh erkannt. 1983 entschied das Bundesverfassungsgericht aufgrund mehrerer Verfassungsbeschwerden zu einer geplanten Volkszählung, dass die informationelle Selbstbestimmung[218] ein Grundrecht ist, welches sich vom Recht auf freie Entfaltung der Persönlichkeit gemäß Art. 2 Abs. 1 GG und der Unantastbarkeit der Menschenwürde gemäß Art.1 GG ableiten lässt.[219] Auf EU-Ebene wird seit 2000, mit Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh), der Schutz von personenbezogenen Daten gewährleistet. Ein modernes und umfassendes Datenschutzregelwerk wurde verbindlich europaweit 2018 mit der DSGVO konstituiert. Die DSGVO ist aus der Notwendigkeit entstanden, die schnellen weltweiten technischen Entwicklungen im Bereich der Datenverarbeitung umfassend zu regulieren. Fraglich ist aber, ob sie imstande ist, die Entwicklungen im Bereich von BCI mitabzudecken. Nachfolgend soll darum eine umfassende Analyse der relevanten DSGVO-Artikel vorgenommen werden, um anhand der Ergebnisse die Möglichkeit der Regulierung von BCI bewerten zu können. Eine ähnliche Betrachtung von BCI findet sich bis dato nur sehr grundlegend

217 *Boehme-Neßler,* International Data Privacy Law 2016, S. 222 (223 f.).
218 *Steinmüller et al.,* BT-Drucksache VI/3826, 1971, S. 88.
219 BVerfG, Urteil v. 15.12.1983 - 1 BvR 209/83, Neue Juristische Wochenschrift 1984, 419.

in Bezug auf die ehemalige europäische Datenschutzrichtlinie,[220] wobei dessen Möglichkeit zur Regulierung von BCI angezweifelt wurde.[221] Die Annahme, dass bestehendes Datenschutzrecht nicht ausreicht, um Smart Human zu schützen, findet sich ebenso im amerikanischen Raum. Auf Grundlage dessen wird argumentiert, dass ein adäquater Schutz nur auf Ebene von Menschenrechten gewährleistet werden kann.[222] In Kalifornien hat diese Diskussion zur kürzlichen Verabschiedung eines Gesetzes zum Schutze von Neurodaten geführt, welches den California Consumer Privacy Act ergänzt.[223] Um die Forschungslücke zu schließen und um eine abschließende Bewertung für den europäischen Raum vorzunehmen, soll mit dieser Arbeit eine vollständige Betrachtung der relevanten aktuellen europäischen Datenschutzvorschriften vorgenommen werden.

220 Amtliche Bezeichnung: Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; Vorgänger der DSGVO.

221 *Hallinan et al.,* Surveillance & Society 2014, S. 55 (S. 66 ff.); *Wahlstrom/Fairweather/Ashman,* Proceedings of the. 12th Int. Ethicomp Conference 2011, S. 471 (473 f.).

222 *Ienca/Andorno,* Life Sciences, Society and Policy 2017, S. 1 (10 ff.).

223 Abrufbar unter: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1223 (abgerufen am 5.1.2025).

F. Prüfung der Anwendbarkeit der DSGVO

I. Art. 2 Abs. 1 DSG1VO: Sachlicher Anwendungsbereich der DSGVO

In Art. 2 DSGVO wird der sachliche Anwendungsbereich der Verordnung und dessen Ausnahmen festgelegt. Während Art. 2 Abs. 1 DSGVO den Geltungsbereich der Norm absteckt und definiert, welche Verarbeitungen erfasst werden, werden in Art. 2 Abs. 2 - 4 DSGVO hingegen Tatbestände aufgezählt, die von der Verordnung ausgenommen sind. Da die dort genannten Ausnahmen für diese Arbeit keine Relevanz besitzen, werden diese hier nicht weiter thematisiert. Es wird sich somit nur auf den konkreten sachlichen Anwendungsbereich in Art. 2 Abs. 1 DSGVO konzentriert.

Art. 2 Abs. 1 DSGVO besagt, dass die Verordnung dann gilt, wenn eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten vorliegt. Ergänzt wird dies durch die Hinzunahme von nicht-automatisierten Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Dem folgend fordert ErwG. 15 eine Technologieneutralität der DSGVO, da das Risiko einer Umgehung der Vorschriften nur eingedämmt werden kann, wenn diese nicht von der verwendeten Technik abhängig gemacht werden.

II. Art. 4 Abs. 1 DSGVO: Personenbezogene Daten

Der Anwendungsbereich der DSGVO ist gemäß Art. 2 Abs. 1 DSGVO eröffnet, wenn eine Verarbeitung von personenbezogenen Daten vorliegt. Dabei ist der Begriff „Daten" nach herrschender Meinung weit auszulegen.[224] Personenbezogene Daten sind i.S.v. Art. 4 Abs. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Demnach sind mit Informationen jegliche objektive Tatsachen (Geburtsort, Name, Vermögensverhältnisse etc.), als auch subjektive Einschätzungen (Bewertungen, Urteile, Scorings etc.)[225] und individuelle Merkmale

224 *Ernst* (2021), Art. 4 Rn. 3*;* EuGH, Urt. v. 7.5.2009 – C-553/07, EuZW 2009, 546 (549); *Schefzig*, DSRITB 2014, S. 103 (104); *Art.-29-Gruppe*, WP 136, 2007, S. 4.

225 *Klabunde* (2018), Art. 4 Rn. 7*; Art.-29-Gruppe*, WP 136, 2007, S. 7.

(Meinungen, Werte, Beziehungen etc.) gemeint.[226] Dabei ist es völlig egal, in welcher Form diese Informationen vorliegen und wie diese gespeichert werden.[227] Der Personenbezug dieser Informationen kann sich dabei entweder alternativ oder kumuliert durch Inhalts-, Zweck- oder Ergebniselemente ergeben.[228] Ein Inhaltselement liegt vor, wenn sich Informationen direkt auf eine bestimmte Person beziehen (Patientenakte, Personalakte etc.), ein Zweckelement liegt vor, wenn die Informationen genutzt werden können, um Auswirkungen für eine bestimmte Person herbeizuführen (z.B. kann die Zuordnung einer Telefonnummer zu einem Mitarbeiter vorgenommen werden, um zu überprüfen, mit wem dieser telefoniert hat) und ein Ergebniselement liegt vor, wenn die Informationen unter Berücksichtigung aller Umstände ggf. eine Auswirkung auf die Rechte und Interessen einer bestimmten Person haben könnten (z.B. die Satellitenortung von Firmenfahrzeugen zum Zweck der Optimierung von Geschäftsprozessen, kann auch genutzt werden, um Mitarbeiter zu überwachen).[229]

Voraussetzung für das Vorliegen solcher personenbezogenen Daten ist, dass diese sich auf eine identifizierte oder identifizierbare Person beziehen. Als identifiziert gilt eine Person dann, wenn die vorhandene Information unmittelbar zur Feststellung der Identität führt.[230] Diese direkte Identifizierung kann bspw. kontextbedingt durch einen Namen gewährleistet werden.[231] Ausschlaggebend ist, dass die Person durch die Information vollkommen ausgesondert werden kann.[232] Als identifizierbar gilt eine Person im Gegensatz dazu, wenn eine Information lediglich indirekt, also durch Verknüpfung mit anderen Informationen, zur Feststellung ihrer Identität führen kann.[233] Nach Art. 4 Nr. 1 DSGVO ist dies gegeben, wenn eine Person, direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Bei der Einschätzung, ob eine solche

226 *Klar/Kühling* (2020), Art. 4 Nr. 1 Rn. 8.
227 *Arning/Rothkegel* (2019), Art. 4 Rn. 7.
228 *Art.-29-Gruppe*, WP 136, 2007, S. 11 ff.
229 Ebenda.
230 EuGH, Urt. v. 19.10.2016 – C-582/14, NVwZ 2017, 213 (214).
231 *Art.-29-Gruppe*, WP 136, 2007, S. 15.
232 *Schantz* (2017), Rn. 291.
233 *Arning/Rothkegel* (2019), Art. 4 Rn. 30.

Zuordnung möglich ist, ergänzt ErwG. 26 dies dahingehend, dass alle Mittel auf Grundlage der verfügbaren Technologie und der technologischen Entwicklung zu berücksichtigen sind, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen, unter Berücksichtigung der Kosten und des Zeitaufwandes, wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Der EuGH konkretisierte dies und stellte fest, dass sich nicht alle Mittel und Informationen, die zur Identifizierung der Person notwendig sind, in den Händen einer Person befinden müssen, um den Tatbestand zu erfüllen.[234] Die verantwortliche Stelle ist somit dazu angehalten, sich auch die Mittel und Informationen zuzurechnen, die von Dritten genutzt werden können, um eine Person zu identifizieren.[235] Beschränkt wird diese mögliche Verknüpfung von Informationen und die Nutzung von Mitteln nur dadurch, dass diese rechtlich zulässig sein muss und der Zugriff auf die Informationen und Mittel Dritter vernünftigerweise vorgenommen werden können muss.[236] Wichtig dabei ist, dass der Personenbezug nicht unbedingt tatsächlich hergestellt werden muss, sondern die alleinige Möglichkeit reicht schon aus, damit eine Identifizierbarkeit i.S.v. Art. 4 Abs. 1 DSGVO vorliegt.[237]

III. Art. 4 Abs. 2 DSGVO: Verarbeitung

Damit der sachliche Anwendungsbereich gemäß Art. 2 Abs. 1 DSGVO tatsächlich eröffnet ist, ist es notwendig, dass diese personenbezogenen Daten von identifizierten oder identifizierbaren natürlichen Personen auch verarbeitet werden. Gemäß Art. 4 Abs. 2 DSGVO liegt eine Verarbeitung dann vor, wenn ein Vorgang, der im Zusammenhang mit personenbezogenen Daten steht, mit oder ohne automatisierte Verfahren ausgeführt wird. Diese Legaldefinition zielt darauf ab, den Begriff der „Verarbeitung" sehr weit auszulegen, sodass jegliche konkrete Handlung, die in irgendeiner Art und Weise mit personenbezogenen Daten zu tun hat und auf egal welcher Art und Weise tatsächlich ausgeführt wird, unter dieser Definition zu subsumieren ist.[238] Die konkrete Benennung von solchen Vorgängen in

234 EuGH, Urt. v. 19.10.2016 – C-582/14, NVwZ 2017, 213 (215).
235 *Karg* (2019), Art. 4 Rn. 61; *Arning/Rothkegel* (2019), Art. 4 Rn. 35; Brink/Eckhardt, ZD 2015, S. 205 (211).
236 EuGH, Urt. v. 19.10.2016 – C-582/14, NVwZ 2017, 213 (215).
237 *Karg* (2019), Art. 4 Rn. 62.
238 *Klabunde* (2018), Art. 4 Rn. 22 f.; *Ernst* (2021), Art. 4 Rn. 21 f.

Art. 4 Abs. 2 DSGVO ist demnach nicht als abschließend, sondern nur als bespielhaft zu verstehen.[239]

IV. Wesensdaten als personenbezogene Daten

Um festzustellen, ob Wesensdaten personenbezogene Daten i.S.v. Art. 4 Abs.1 u. 2 DSGVO sind, bedarf es einer Aufteilung der zuvor definierten Wesensdaten in ihre zwei initialen Bestandteile (neurologische Rohdaten und die Auswertung dieser Daten), damit diese gesondert voneinander betrachtet werden können.

Neurologische Rohdaten sind keine Daten, die eine direkte Identifikation von Personen ermöglichen. Allerdings kann eine Kopplung mit anderen Daten dazu führen, dass die Person theoretisch identifizierbar wird. BCI werden derzeit hauptsächlich in Forschungseinrichtungen genutzt. Hier könnte eine Zuordnung der neurologischen Rohdaten zu der jeweiligen Testperson eine Identifizierung ermöglichen. Sollten BCI zukünftig für den privaten Gebrauch genutzt werden, wird hier auch eine Zuordnung zu einem Nutzerkonto und/oder einer Gerätenummer der jeweiligen Hardware möglich sein, womit die nutzende Person identifizierbar ist. Unter Berücksichtigung der dazu notwendigen Mittel, der verfügbaren Technologie und des Aufwandes, ist eine Identifizierbarkeit gemäß Art. 4 Abs. 1 DSGVO eindeutig gegeben. Der konkrete Personenbezug ergibt sich bei neurologischen Rohdaten aus einem Inhaltselement, wenn die Zuordnung zu einer Testperson oder Hardware bereits stattgefunden hat und aus einem Zweckelement, da eine Zuordnung der Daten zu einer bestimmten Person vorgenommen werden kann, um damit den Zweck der letztendlichen Auswertung der Daten (bspw. um bestimmte Outputs zu generieren) zu ermöglichen. Ergänzend könnte auch ein Ergebniselement vorliegen, wenn die neurologischen Rohdaten bspw. für die Steuerung eines automatisierten Rollstuhls erhoben werden, aber theoretisch auch dafür genutzt werden könnten, andere Auswertungen mit anderer Aussagekraft vorzunehmen. Neurologische Rohdaten sind demnach eindeutig als personenbezogene Daten i.S.v. Art. 4 Abs. 1 DSGVO zu definieren.

Bei den Auswertungen der neurologischen Rohdaten, die eine fallabhängige Aussagekraft besitzen, besteht die Möglichkeit, eine direkte und eindeutige Identifikation einer bestimmten Person zu ermöglichen. Hier

239 *Reimer* (2018), Art. 4 Rn. 53.

ist besonders der mögliche Einsatz bei Authentifizierungs- bzw. Identifizierungsmaßnahmen zu erwähnen,[240] wobei zwangsläufig Informationen vorliegen, die sich auf eine identifizierte Person beziehen. Bedenkt man das Informationsschöpfungspotenzial von BCI-Daten und die in Kapitel D.I. bereits zusammengefassten existierenden Möglichkeiten, ist eine direkte Identifikation von Nutzern, auch außerhalb von Authentifizierungs- bzw. Identifizierungsmaßnahmen, in Zukunft denkbar und wahrscheinlich. Daneben können sich diese Auswertungen ebenso auf identifizierbare Personen beziehen. Auch hier könnte eine Kopplung mit anderen Daten dazu führen, dass eine bestimmte Person ausgesondert werden kann. Wie bei den neurologischen Rohdaten ist bspw. eine Zuordnung der konkreten Auswertungen zu der jeweiligen Testperson oder einer spezifischen Gerätenummer möglich. Des Weiteren können auch die Auswertungen an sich eine Identifizierbarkeit ermöglichen. Hier ist besonders die Ermittlung des Standortes und die Erzeugung von Bankdaten erwähnenswert.[241] Unter Berücksichtigung der dazu notwendigen Mittel, der verfügbaren Technologie und des Aufwandes, ist eine Identifizierung und Identifizierbarkeit bei der Auswertung von neurologischen Rohdaten gemäß Art. 4 Abs. 1 DSGVO gegeben. Der konkrete Personenbezug kann sich hierbei, je nach Auswertung, aus einem Inhaltselement, Zweckelement oder Ergebniselement ergeben. Ein Inhaltselement liegt vor, wenn die Auswertung als Authentifizierungs- bzw. Identifizierungsmaßnahme genutzt wird, womit eine Person eindeutig identifiziert wird. Ein Zweckelement ist in einigen Fällen denkbar, da eine Zuordnung der Auswertungen zu einer bestimmten Person vorgenommen werden kann, um z.B. zu überprüfen, ob stereotype Vorurteile vorliegen[242] oder ob einer politischen Rede zugestimmt wird.[243] Damit könnten weitreichende Auswirkungen für die Person herbeigeführt werden. Das Ergebniselement ergibt sich bspw. bei Auswertungen, die für die Steuerung von Smart Home-Anwendungen erzeugt werden, aber ebenso dafür genutzt werden können, den Nutzer zu überwachen. Die Auswertungen der neurologischen Rohdaten sind demnach ebenso eindeutig als personenbezogene Daten i.S.v. Art. 4 Abs. 1 DSGVO zu definieren.

240 *Landau/Puzis/Nissim,* AMC Computing Surveys 2020, S. 1 (12 ff.).
241 *Martinovic et al.,* Proceedings of the 21st USENIX Security Symposium 2012, S. 1 (5 ff.).
242 *Knutson et al.,* Human Brain Mapping 2007, S. 915 (927).
243 *Vecchiato et al.,* 31st Annual International Conference of the IEEE EMBS 2009, S. 57 (59f.).

Damit der Anwendungsbereich der DSGVO vollständig eröffnet ist, muss auch eine Verarbeitung der Wesensdaten vorliegen. Da BCI neurologische Rohdaten aufzeichnen und mithilfe einer KI auswerten, liegt ohne Zweifel ein konkreter Vorgang vor, der im Zusammenhang mit personenbezogenen Daten steht und mit Hilfe von automatisierten Verfahren tatsächlich ausgeführt wird. Damit kann festgehalten werden, dass die Verarbeitung von Wesensdaten mittels BCI bereits vom sachlichen Anwendungsbereich des Art. 2 Abs. 1 DSGVO erfasst ist.

G. Prüfung, ob die DSGVO einen ausreichenden Schutz gewährleistet

I. Besondere Kategorien von personenbezogenen Daten

1. Analyse von Art. 9 Abs. 1 DSGVO

In Art. 9 Abs. 1 DSGVO werden jene Datenkategorien aufgeführt, die aufgrund ihrer gewöhnlichen Aussagekraft als besonders sensitiv einzustufen sind. Diese besonderen Kategorien von personenbezogenen Daten (im Folgenden auch sensitive Daten) sind von höchstpersönlicher Natur und können in einigen Fällen eine präzise und weitreichende Identifizierung der betroffenen Person gewährleisten.[244] Erwägungsgrund 51 S. 1 unterstreicht diese Einstufung, indem der besondere Bezug zu den Grundrechten und Grundfreiheiten der betroffenen Person hergestellt wird und legt demnach fest, dass eine Verarbeitung dieser Daten mit einem erheblichen Risiko für eben jene Grundrechte und Grundfreiheiten verbunden ist. Dem folgend ist die Verarbeitung dieser besonderen Kategorien von personenbezogenen Daten grundsätzlich verboten, es sei denn ein Ausnahmetatbestand gemäß Art. 9 Abs. 2 DSGVO liegt vor. Damit bleibt die DSGVO ihrem risikobasierten Ansatz bei der Verarbeitung von sensitiven Daten treu,[245] womit gegenüber den Erlaubnistatbeständen von Art. 6 Abs. 1 UAbs. 1 DSGVO eine teilweise Sperrwirkung entfaltet wird, die insbesondere das berechtigte Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO bei sensiblen Daten ausschließt.[246]

Art. 9 Abs. 1 DSGVO spricht Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, aber auch genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, den Status von besonderen Kategorien von personenbezogenen Daten zu. Al-

244 *Frenzel* (2021), Art. 9 Rn. 6.
245 *Weichert* (2020), Art. 9 Rn. 4.
246 *Schulz* (2018), Art. 9 Rn. 5.

lerdings werden diese Datenkategorien nicht alle abschließend definiert. Um eine Einordnung von Wesensdaten in den Regelungsbereich des Art. 9 DSGVO vorzunehmen, wird eine Analyse und Abgrenzung dieser sensitiven Daten notwendig sein. Besonders zu erwähnen ist hierbei, dass Art. 9 Abs. 1 DSGVO eine zweigleisige Schutzwürdigkeit der Datenkategorien vorsieht.[247] Bei Daten zu der rassischen und ethnischen Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen oder der Gewerkschaftszugehörigkeit ist ein Schutz gewährleistet, wenn aus ihnen die konkreten Eigenschaften „hervorgehen".[248] Dafür ist es ausreichend, wenn aus den Daten mittelbar die relevante Eigenschaft gefolgert werden kann.[249] Die Auslegung, ob ein solches Hervorgehen vorliegt, ist dabei großzügig vorzunehmen,[250] sodass es auch nicht erforderlich ist, dass die abgeleiteten Eigenschaften tatsächlich richtig sein müssen.[251] Im Gegensatz dazu unterliegen genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person pauschal dem Schutz des Art. 9 DSGVO.[252]

a. Rassische und ethnische Herkunft

Unter Daten zur rassischen und ethnischen Herkunft sind Merkmale der betroffenen Person zu subsumieren, die einen Rückschluss auf dessen Herkunft[253] und Zugehörigkeit zu einer bestimmten Bevölkerungsgruppe zulassen.[254] Dazu zählt insbesondere die Hautfarbe und andere phänotypische, körperliche Unterschiede,[255] aber auch spezifische regional beschränkte Sprachen[256] oder andere kulturelle und historische Eigenschaften.[257] Na-

247 *Schiff* (2018), Art. 9 Rn. 13; *Schulz* (2018), Art. 9 Rn. 13; *Petri* (2019), Art. 9 Rn. 12; Anderer Meinung: *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1594 u. 1598); *McCullagh,* Journal of International Commercial Law and Technology 2007, S. 190 (192 ff.); *Frenzel* (2021), Art. 9 Rn. 8.
248 *Schiff* (2018), Art. 9 Rn. 13; *Schulz* (2018), Art. 9 Rn. 13.
249 *Frenzel* (2021), Art. 9 Rn. 8.
250 *Schiff* (2018), Art. 9 Rn. 13.
251 *Schneider,* ZD 2017, S. 303 (305).
252 *Schiff* (2018), Art. 9 Rn. 13.
253 *Mester* (2019), Art. 9 Rn. 7.
254 *Greve* (2020), Art. 9 Rn. 7.
255 Ebenda.
256 *Schulz* (2018), Art. 9 Rn. 14.
257 *Schiff* (2018), Art. 9 Rn. 15.

men, Geburts- und Wohnorte können zwar ein Indiz für eine ethnische Zugehörigkeit sein,[258] allerdings sind diese oftmals willkürlichen Entscheidungen unterworfen, sodass diese Informationen nur im Ausnahmefall unter Daten zur rassischen und ethnischen Herkunft zu subsumieren sind.[259]

b. Politische Meinung

Daten, aus denen die politische Meinung der betroffenen Person hervorgehen, sind ebenso durch Art. 9 Abs. 1 DSGVO besonders geschützt. Wie weit die politische Natur von Daten zu definieren ist, ist allerdings umstritten.[260] Aus der konkreten Mitgliedschaft bei einer Partei, das Abonnement einer klar parteipolitisch-ausgerichteten Zeitung[261] und aus der expliziten Tätigkeit als politischer Akteur[262] geht eindeutig die politische Meinung der betroffenen Person hervor. Bei der Teilnahme an Demonstrationen oder politischen Veranstaltungen, Likes o.Ä. für Postings von politischen Parteien[263] oder nicht konkret politischen Tätigkeiten bei einer Partei,[264] ist nicht zwangsläufig ein zweifelfreies Hervorgehen der politischen Meinung gegeben.[265] Doch ist das Hervorgehen der Information nicht vollständig ausgeschlossen. Die Möglichkeit besteht, dass die kumulierten Tätigkeiten, aus denen im Einzelfall für gewöhnlich nicht die politische Meinung hervorgeht, sehr wohl genaue Rückschlüsse zulassen. Deutlich wurde dies bspw. im Facebook-Skandal rundum Cambridge Analytica,[266] bei dem Microtargeting, also das personen- und interessenspezifische Schalten von Inhalten,[267] angewandt wurde. Anhand der kumulierten Tätigkeiten der betroffenen Person auf Social Media-Plattformen können Wahlprognosen und Scores ermittelt werden, um individuelle, auf Gruppen und Einzel-

258 *Schneider,* ZD 2017, S. 303 (305).
259 *Weichert* (2020), Art. 9 Rn. 26.
260 Großzügige Auslegung: *Mester* (2019), Art. 9 Rn. 8; *Weichert* (2020), Art. 9 Rn. 27; *Greve* (2020), Art. 9 Rn. 8; *Kampert* (2018), Ar. 9 Rn. 8; gemäßigte Auslegung: *Schiff* (2018), Art. 9 Rn. 19 ff.; enge Auslegung: *Schulz* (2018), Art. 9 Rn. 14.
261 *Mester* (2019), Art. 9 Rn. 8.
262 *Schulz* (2018), Art. 9 Rn. 14.
263 *Schiff* (2018), Art. 9 Rn. 20.
264 *Schulz* (2018), Art. 9 Rn. 14 schließt bspw. die Tätigkeit im Sekretariat oder in der IT-Administration aus.
265 *Schiff* (2018), Art. 9 Rn. 21.
266 *Chester/Montgomery,* Internet Policy Review 2017, S. 1 (7).
267 *Zuiderveen Borgesius et al.,* Utrecht Law Review 2018, S. 82 (82).

personen zugeschnittene Maßnahmen zu entwickeln, welche die Stimmenvergabe bei Wahlen beeinflussen können.[268] Um dem Schutzzweck des Art. 9 DSGVO zu entsprechen, ist es somit notwendig, das Hervorgehen der politischen Meinung genau zu prüfen. Die Auslegung, ob ein solches Hervorgehen vorliegt, ist dabei großzügig vorzunehmen,[269] sodass es auch nicht erforderlich ist, dass die abgeleiteten Eigenschaften tatsächlich richtig sein müssen.[270] Auf der anderen Seite ist aber auch eine Supererogation zu vermeiden, durch welche unnötig viele Daten und Datenkategorien unter Art. 9 Abs. 1 DSGVO subsumiert werden würden, bei denen kein zweifelsfreies Hervorgehen der politischen Meinung vorliegt.

c. Religiöse und weltanschauliche Überzeugung

Bezugnehmend auf die Diskriminierungsverbote aus Art. 21 GRCh (Gebot religiöser Vielfalt) und Art. 10 GRCh (Glaubens- und Gewissensfreiheit), sieht die DSGVO einen besonderen Schutz von Daten vor, aus denen die religiöse und weltanschauliche Überzeugung hervorgeht.[271] Die Abgrenzung zur politischen Meinung liegt darin, dass sich die politische Meinung auf aktuelle Ereignisse und Fragestellungen konzentriert und somit die demokratische Teilnahme des Einzelnen umschreibt, während sich die religiöse und weltanschauliche Überzeugung auf grundsätzliche, sinnstiftende Fragen zum Leben und des Daseins bezieht.[272] Auch untereinander lassen sich die Begriffe differenzieren, da sich religiöse Überzeugungen durch einen transzendentalen Bezug kennzeichnen, während dieser Bezug zur Transzendenz bei der weltanschaulichen Überzeugung nicht gegeben ist.[273] Damit soll gewährleistet werden, dass sowohl die großen Weltreligionen (Christentum, Islam, Buddhismus, Hinduismus), Naturreligionen und Sekten als auch Atheismus und weitere davon abweichende philosophische Konstrukte, von Art. 9 Abs. 1 DSGVO geschützt werden.[274] Wie weit dieser

268 *Christl,* Aus Politik und Zeitgeschichte 2019, S. 42 (46 ff.).
269 *Schiff* (2018), Art. 9 Rn. 13.
270 *Schneider,* ZD 2017, S. 303 (305).
271 *Weichert* (2020), Art. 9 Rn. 28; *Greve* (2020), Art. 9 Rn. 9.
272 *Weichert* (2020), Art. 9 Rn. 28; *Kampert* (2018), Ar. 9 Rn. 9.
273 *Schiff* (2018), Art. 9 Rn. 24.
274 *Kampert* (2018), Ar. 9 Rn. 9.

Schutz geht, ist allerdings umstritten.[275] Auf Seiten der religiösen Überzeugung sind Konfessionszugehörigkeit, Mitgliedschaft in einer Kirche, Besuch von Gottesdiensten und weitere explizite Tätigkeiten und Informationen mit Bezug zu einer Religion eindeutig unter Art. 9 Abs, 1 DSGVO zu subsumieren.[276] Das Tragen von religiösen Symbolen, religiöser Kleidung oder der Besitz von Devotionalien ist allerdings nicht immer als sensibles Datum i.S.v. Art. 9 Abs. 1 DSGVO zu sehen.[277] Bei der weltanschaulichen Überzeugung ist es wichtig, auf die Gesamtsicht der betroffenen Person abzustellen und nicht jede einzelne Überzeugung und Einstellung zu berücksichtigen.[278] Somit ist die Tatsache, dass die betroffene Person Vegetarier oder Pazifist ist, nicht unbedingt als Datum zu sehen, aus dem die weltanschauliche Überzeugung hervorgeht,[279] da damit im Normalfall nur Teilaspekte der Gesamtsicht beschrieben werden. Im Gegensatz dazu sind eindeutige Ideologien wie Kommunismus, Faschismus[280] oder die Mitgliedschaft in ethischen Gemeinschaften wie bspw. der Freimaurer,[281] als Daten zur weltanschaulichen Überzeugung zu definieren.

d. Gewerkschaftszugehörigkeit

Vor dem Hintergrund des Art. 25 GRCh (Koalitionsfreiheit) und Art. 31 GRCh (Diskriminierungsverbot) wurden auch Daten, aus denen die Gewerkschaftszugehörigkeit hervorgehen, in den Korpus des Art. 9 Abs. 1 DSGVO aufgenommen.[282] Damit soll eine mögliche Diskriminierung von Arbeitnehmer durch Arbeitgeber und auf dem Arbeitsmarkt verhindert werden.[283] Somit fallen sowohl die Mitgliedschaft in einer entsprechenden Gewerkschaft/Organisation als auch Tätigkeiten, die eine Mitgliedschaft in einer solchen Organisation vermuten lassen, unter den Schutz des

275 Großzügige Auslegung: *Greve* (2020), Art. 9 Rn. 8; *Kampert* (2018), Ar. 9 Rn. 9; gemäßigte Auslegung: *Mester* (2019), Art. 9 Rn. 10 f.; *Wedde* (2020), Art. 9 Rn. 22; enge Auslegung: *Schulz* (2018), Art. 9 Rn. 14.
276 *Wedde* (2020), Art. 9 Rn. 22.
277 *Schulz* (2018), Art. 9 Rn. 14.
278 *Mester* (2019), Art. 9 Rn. 11; *Schulz* (2018), Art. 9 Rn. 14.
279 *Schulz* (2018), *Art. 9 Rn. 14.*
280 *Kampert* (2018), Art. 9 Rn. 9.
281 *Schulz* (2018), Art. 9 Rn. 14.
282 *Albers/Veit* (2020), Art. 9 Rn. 36.
283 *Weichert* (2020), Art. 9 Rn. 30.

Art. 9 Abs. 1 DSGVO.[284] Dafür muss das Datum vor allem einen klaren inhaltlichen Zusammenhang zur Gewerkschaftstätigkeit aufweisen.[285] Das Bekleiden von Funktionen in einer Gewerkschaft und das Engagement in einer eindeutig gewerkschaftsnahen Stiftung sind als Daten i.S.v. Art, 9 Abs.1 DSGVO zu definieren.[286] Das alleinige Abonnement einer Gewerkschaftszeitung oder der Besuch einer Gewerkschaftsveranstaltung sind nicht zwangsläufig Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht.[287] Die Art der Gewerkschaft hat keine Auswirkung auf den Schutz des Datums, sodass es völlig egal ist, ob eine politische oder neutrale Ausrichtung vorliegt.[288]

e. Genetische Daten

In Art. 4 Abs. 13 DSGVO wird eine Legaldefinition für genetische Daten bereitgestellt. Darin wird erläutert, dass personenbezogene Daten zu ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden, als genetische Daten zu definieren sind. ErwG. 34 spezifiziert dies durch die Aufzählung von Chromosomen-, DNS- und RNA-Analysen aber stellt ebenso fest, dass diese Aufzählung nicht erschöpfend ist. Auch die Formulierung „insbesondere" verdeutlicht, dass nicht unbedingt eine Analyse von biologischen Proben vorliegen muss, sondern auch zukünftige Methoden der Genanalyse berücksichtigt werden müssen.[289] Geschützt werden die Ergebnisse der Analyse sowie der zugrundeliegende genetische Code.[290] Somit werden bspw. sowohl spezifische Erbmerkmale zur biologischen Abstammung oder zu Krankheitsdispositionen erfasst als auch Informationen über gewisse Fähigkeiten und Lebensumstände.[291]

284 *Petri* (2019), Art. 9 Rn. 22.
285 *Schulz* (2018), Art. 9 Rn. 14.
286 *Petri* (2019), Art. 9 Rn. 22.
287 *Albers/Veit* (2020), Art. 9 Rn. 37; *Petri* (2019), Art. 9 Rn. 22; anderer Meinung, zumindest was Gewerkschaftsveranstaltungen angeht: *Schiff* (2018), Art. 9 Rn. 26.
288 *Weichert* (2020), Art. 9 Rn. 30.
289 *Petri* (2019), Art. 4 Nr. 13 Rn. 12.
290 Ebenda, Art. 4 Nr. 13 Rn. 13.
291 *Vossenkuhl,* Der Schutz genetischer Daten, 2013, S. 4.

Mit genetischen Daten führt die DSGVO eine neue Schutzkategorie ein, die das genetische Diskriminierungsverbot aus Art. 21 Abs. 1 GRCh aufgreift.[292] Ebenso sollen weitreichende Eingriffe in die Privatsphäre der betroffenen Personen verhindert werden,[293] da genetische Daten für die gesamte Lebenszeit meist unverändert bleiben und die darin festgehaltenen Merkmalen, wie bspw. äußerlich erkennbare sowie innerliche körperliche und seelische Merkmale, somit zu jeder Zeit der betroffenen Person zugerechnet werden können.[294] Eine Anonymisierung ist demnach nicht möglich.[295] Die Genanalyse ermöglicht aber nicht nur die Merkmalszuordnung bei der betroffenen Person, sondern auch bei dessen näheren biologischen Verwandten.[296]

f. Biometrische Daten

Um der Erstellung von umfassenden Persönlichkeitsprofilen entgegenzuwirken, kodifiziert die DSGVO den neuen Schutzbereich der biometrischen Daten.[297] Auch hierzu findet sich eine Legaldefinition in Art. 4 Nr. 14 DSGVO, die besagt, dass Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen der betroffenen Person als biometrische Daten gelten. Da damit alle Daten erfasst werden, die im Bezug zum menschlichen Körper stehen, ist der Schutzbereich zunächst weit gefasst.[298] Allerdings nimmt die Legaldefinition Einschränkungen vor. So ist Voraussetzung für das Vorliegen solcher Daten, dass diese Daten eine eindeutige Identifizierung der natürlichen Person gewährleisten und mit speziellen technischen Verfahren gewonnen wurden.

Eine eindeutige Identifizierung liegt vor, wenn die erhobenen Merkmale einzigartig sind,[299] auch wenn diese Einzigartigkeit nicht weltweit gelten muss.[300] Wichtig ist somit nur, dass eine objektive Unverwechselbarkeit der betroffenen natürlichen Person vorliegen muss.[301] Als Beispiele von

292 *Weichert* (2020), Art. 9 Rn. 31.
293 *Wedde* (2020), Art. 9 Rn. 27.
294 *Weichert* (2020), Art. 4 Nr. 13 Rn. 5.
295 *Schaar*, ZD 2016, S. 224 (225).
296 *Weichert* (2020), Art. 4 Nr. 13 Rn. 5.
297 Ebenda, Art. 9 Rn. 32.
298 *Kampert* (2018), Art. 4 Rn. 185.
299 *Weichert* (2020), Art. 4 Nr. 14 Rn. 2.
300 *Ernst* (2021), Art. 4 Rn. 101.
301 EuGH, Urt. v. 17.10.2013 – C-291/12, ZD 2013, 608 (609).

Daten, die eine eindeutige Identifizierung ermöglichen, nennt Art. 4 Nr. 14 DSGVO Gesichtsbilder oder daktyloskopische Daten (Fingerabdruckverfahren). Die Aufzählung ist jedoch nicht erschöpfend. Weitere Beispiele sind Iris-, Stimmen- und Venenerkennung,[302] sowie die Gesichtserkennung.[303] Gesichts- bzw. Lichtbilder gelten nur dann als biometrische Daten, wenn diese mit speziellen technischen Mitteln verarbeitet wurden, um die eindeutige Identifizierung der natürlichen Person zu gewährleisten.[304] Somit sind Lichtbilder in amtlichen Ausweisdokumenten wie Pässen oder Personalausweisen als biometrische Daten zu definieren,[305] Bilder auf Semestertickets oder Mitgliedsausweisen allerdings nicht.

Auch die speziellen technischen Verfahren, mit denen die eindeutige Identifizierung der betroffenen natürlichen Person vorgenommen werden kann, benennt Art. 4 Nr. 14 DSGVO nicht abschließend. Es werden lediglich die derzeit gängigen biometrischen Verfahren, also die Gesichtserkennung und das Fingerabdruckverfahren, explizit erwähnt, womit aber kein Ausschluss von zukünftigen oder vergleichbaren Verfahren mit gleicher Wirkung stattfindet.[306]

g. Gesundheitsdaten

Die Schutzbereiche der Art. 2, 3 GRCh (Schutz von Leben und Gesundheit) und des Art. 35 GRCh (Gesundheitsschutz) aufgreifend, wurden auch Gesundheitsdaten in Art. 9 Abs. 1 DSGVO verankert.[307] Gesundheitsdaten werden durch Art. 4 Nr. 15 DSGVO als Daten definiert, die sich auf die körperliche oder geistige Gesundheit der betroffenen Person beziehen und aus denen der entsprechende Gesundheitszustand hervorgeht. ErwG. 35 verdeutlicht, dass es dabei egal ist, ob aus den Informationen frühere, gegenwärtige und künftige körperliche oder geistige Gesundheitszustände der betroffenen Person hervorgehen. Davon werden auch jene Informationen erfasst, die im Zuge von Gesundheitsdienstleistungen i.S.d. Richt-

302 *Schulz* (2018), Art. 9 Rn. 14.
303 *Art.-29-Gruppe,* WP 192, 2012, S. 1.
304 *Schild* (2020), Art. 4 Rn. 141; *Ernst* (2021), Art. 4 Rn. 103.
305 *Schild* (2020), Art. 4 Rn. 141.
306 *Ernst* (2021), Art. 4 Rn. 102.
307 *Weichert* (2020), Art. 9 Rn. 34.

linie 2011/24/EU[308] anfallen, sowie Kennzeichnungen (durch Nummern, Symbole o.ä.), die die natürliche Person für gesundheitliche Zwecke eindeutig identifizieren. Zusammenfassend können alle Informationen, etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person, als Gesundheitsdaten gelten.

Daten, die sich direkt auf den körperlichen und geistigen Gesundheitszustand der betroffenen Person beziehen sind bspw. Diagnosen, Befunde, Drogenkonsum und -missbrauch,[309] Operationen, Impfungen[310] und Einstufungen bspw. als Schwerbehinderter.[311] Daten, aus denen der Gesundheitszustand der betroffenen Person hervorgeht, können vielfältig sein. Hierunter sind vor allem Aufenthalte in bestimmten medizinischen Einrichtungen, die Teilnahme an Selbsthilfegruppen[312] oder in einigen Fällen auch die Informationen über einen Arztbesuch[313] zu subsumieren. Ebenso können Gesundheitsdaten durch die Verknüpfung von verschiedenen Daten, die allein jeweils keine Aussage über den Gesundheitszustand machen, entstehen.[314] Besonders beispielhaft sind hier Wearables, wie Fitness-Tracker und Smart-Watches, da die mithilfe dessen erhobenen Schrittzahlen bspw. Rückschlüsse auf die Herz-Kreislauf-Gesundheit zulassen.[315]

h. Daten zum Sexualleben und der sexuellen Orientierung

Erneut das Diskriminierungsverbot aus Art. 21 Abs. 1 GRCh aufgreifend, zählt die DSGVO auch Daten zum Sexualleben und der sexuellen Orientierung zu den sensitiven Daten.[316] Zu den Daten zum Sexualleben gehören vor allem Informationen zu Sexualpartner, sexuellen Vorlieben und über ausgeübte sexuelle Praktiken.[317] Hierunter können auch Bestellungen

308 Richtlinie über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsvorsorge.
309 *Ernst* (2021), Art. 4 Rn. 108; anderer Meinung: *Frenzel* (2021), Art. 9 Rn. 15.
310 *Weichert* (2020), Art. 9 Rn. 39.
311 *Gola/Schomerus (2012)*, § 3 Rn. 56 a.
312 *Ernst* (2021), Art. 4 Rn. 108; *Weichert* (2020), Art. 9 Rn. 39.
313 *Schulz* (2018), Art. 9 Rn. 14.
314 *Frenzel* (2021), Art. 9 Rn. 15.
315 *Ernst* (2021), Art. 4 Rn. 110.
316 *Greve* (2020), Art. 9 Rn. 13.
317 *Schiff* (2018), Art. 9 Rn. 30.

in Sex-Shops,[318] der Konsum von pornografischen Inhalten[319] und die berufliche Tätigkeit im Prostitutionsgewerbe fallen.[320] Die sexuelle Orientierung stellt eine spezielle Unterkategorie des Sexuallebens dar.[321] Da die sexuelle Orientierung aber oftmals noch ein Diskriminierungsgrund ist, wurden diese Daten explizit gesondert in den Verbotsbereich des Art. 9 Abs. 1 DSGVO aufgenommen.[322] Umfasst von diesem Schutzbereich sind insbesondere Informationen über das bevorzugte Geschlecht von Sexualpartnern, über eine Hetero-, Bi-, Homo- oder sonstige Sexualität und auch Informationen zu Geschlechtsumwandelungen.[323]

2. Kontext- oder zweckabhängige Definition von besonderen Kategorien von personenbezogenen Daten

Durch die vorausgegangene Analyse des Art. 9 Abs. 1 DSGVO konnten die einzelnen besonderen Kategorien von personenbezogenen Daten voneinander abgegrenzt werden. Daraus geht allerdings noch nicht hervor, wann genau ein bestimmtes personenbezogenes Datum als eine besondere Kategorie von personenbezogenen Daten zu definieren ist. Besonders bei Daten, die intrinsisch keine sensitive Aussage beinhalten, ist dies relevant.

Wie bereits dargelegt, sieht Art. 9 Abs. 1 DSGVO eine zweigleisige Schutzwürdigkeit der Datenkategorien vor.[324] Bei Daten zu der rassischen und ethnischen Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen oder der Gewerkschaftszugehörigkeit ist ein Schutz gewährleistet, wenn aus ihnen die konkreten Eigenschaften „hervorgehen".[325] Dafür ist es ausreichend, wenn aus den Daten mittelbar die relevante Eigenschaft gefolgert werden kann.[326] Die Auslegung, ob ein sol-

318 *Plath* (2018), Art. 9 Rn. 10; anderer Meinung: *Schulz* (2018), Art. 9 Rn. 14.
319 *Schiff* (2018), Art. 9 Rn. 31; anderer Meinung: *Schulz* (2018), Art. 9 Rn. 14.
320 *Boehme-Neßler,* DuD 2019, S. 342 (343).
321 *Kampert* (2018), Art. 9 Rn. 11.
322 *Schiff* (2018), Art. 9 Rn. 30.
323 *Wedde* (2020), Art. 9 Rn. 45.
324 *Schiff* (2018), Art. 9 Rn. 13; *Schulz* (2018), Art. 9 Rn. 13; *Petri* (2019), Art. 9 Rn. 12; Anderer Meinung: *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1594 u. 1598); *McCullagh,* Journal of International Commercial Law and Technology 2007, S. 190 (192 ff.); *Frenzel* (2021), Art. 9 Rn. 8.
325 *Schiff* (2018), Art. 9 Rn. 13; *Schulz* (2018), Art. 9 Rn. 13.
326 *Frenzel* (2021), Art. 9 Rn. 8.

ches Hervorgehen vorliegt, ist dabei großzügig vorzunehmen,[327] sodass es auch nicht erforderlich ist, dass die abgeleiteten Eigenschaften tatsächlich richtig sein müssen.[328] Im Gegensatz dazu unterfallen genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person pauschal dem Schutz des Art. 9 DSGVO, da diese inhärent sensitiv sind.[329]

Diese Unterscheidung wirft allerdings die Frage auf, ab wann genau aus einem Datum genug Sensitivität hervorgeht, sodass dieses als besondere Kategorie von personenbezogenen Daten definiert werden muss.[330] Aus Likes für Beiträge auf einer Social Media-Plattform könnte bspw. statistisch eine politische Meinung hervorgehen, allerdings sind damit nicht alle Likes gleich als besondere Kategorien von personenbezogenen Daten zu definieren.[331] Diese Frage lässt sich auch grundsätzlich auf Art. 9 Abs 1 DSGVO anwenden. Unabhängig von der möglichen gesetzlichen Unterscheidung der Schutzwürdigkeit,[332] ist demnach offen, welche Kriterien vorliegen müssen, damit ein Datum unter Art. 9 Abs. 1 DSGVO zu subsumieren ist. Eine Diagnose bspw. ist eindeutig als Gesundheitsdatum zu definieren, bei Daten zur täglichen Ernährung einer Person ist wiederum fraglich, ab wann diese tatsächlich sensitive Aussagen über den Gesundheitszustand zulassen und ab wann diese dann ebenfalls als Gesundheitsdatum gelten.[333]

Um eine Bestimmung von besonderen Kategorien von personenbezogenen Daten zu gewährleisten, ist demnach entweder auf den Verarbeitungskontext oder auf den Verarbeitungszweck/die Verarbeitungsabsicht

327 *Schiff* (2018), Art. 9 Rn. 13.
328 *Schneider,* ZD 2017, S. 303 (305).
329 *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 4; *Schiff* (2018), Art. 9 Rn. 13.
330 *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 4; *Schiff* (2018), Art. 9 Rn. 5; *Frenzel* (2021), Art. 9 Rn. 8.
331 *Albers/Veit* (2020), Art. 9 Rn. 29.
332 Gehen davon aus, dass diese Unterscheidung überhaupt nicht besteht: *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1594 u. 1598); *McCullagh,* Journal of International Commercial Law and Technology 2007, S. 190 (192); *Frenzel* (2021), Art. 9 Rn. 8; Gehen zwar von einer Unterscheidung aus, stellen sich jedoch indirekt die gleiche Frage: *Albers/Veit* (2020), Art. 9 Rn. 29 (nennt als Bsp. Rückschlüsse auf sexuelle Orientierung); *Weichert* (2020), Art. 9 Rn. 22 (nennt als Beispiel Rückschlüsse auf die Gesundheit); *Petri* (2019), Art. 9 Rn. 12 (nennt als Beispiel Rückschlüsse auf die Gesundheit).
333 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1598).

abzustellen.[334] Auf der einen Seite besteht somit eine diesbezüglich kontextabhängige Bestimmung und auf der anderen Seite eine zweckabhängige Bestimmung.[335] Im Nachfolgenden sollen diese Vorgehensweisen jeweils analysiert und kritisch beleuchtet werden. Ebenso soll mit einem Abgleich zur derzeit gängigen Datenschutz-Praxis ermittelt werden, wie die Bestimmung von besonderen Kategorien von personenbezogenen Daten tatsächlich vorgenommen wird. Die Ergebnisse dieser Betrachtung sollen dann genutzt werden, um feststellen zu können, ob Wesensdaten unter Art. 9 Abs. 1 DSGVO zu subsumieren sind.

a. Kontextabhängige Bestimmung

Bei der kontextabhängigen Bestimmung von besonderen Kategorien von personenbezogenen Daten ist der Verarbeitungskontext maßgeblich. Das bedeutet, dass sich die Sensitivität eines Datums aus dem Gesamtzusammenhang der Verarbeitung ergibt.[336] Für die Bewertung dieses Gesamtzusammenhanges ist grundlegend erstmal relevant, zu welchem Zweck die Daten verarbeitet werden, wie die Datenverarbeitung abläuft, mit welcher Technik die Daten verarbeitet werden, ob eine Möglichkeit zur Verknüpfung mit weiteren Daten besteht und an welche Dritten die Daten ggf. übermittelt werden.[337] Bei einer weiten Auslegung des Gesamtzusammenhanges werden auch noch die allgemeinen technischen Möglichkeiten, die der Verantwortliche hat[338] und wie sich das Auswertungspotential der Daten in Zukunft verändern könnte, berücksichtigt.[339] Wenn nicht bereits eine inhärente Sensitivität des Datums vorliegt, soll die Bewertung des Gesamtzusammenhanges aufzeigen, mit welcher Wahrscheinlichkeit sich eine sensitive Information bei dem jeweiligen Verarbeitungskontext aus den

334 *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 4; *Schiff* (2018), Art. 9 Rn. 5; *Frenzel* (2021), Art. 9 Rn. 8.
335 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1590 ff.); *McCullagh,* Journal of International Commercial Law and Technology 2007, S. 190 (198 ff.); *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 4; *Albers/Veit* (2020), Art. 9 Rn. 18 ff.
336 *Petri* (2019), Art. 9 Rn. 11.
337 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1591); *Albers/Veit* (2020), Art. 9 Rn. 30.
338 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1591).
339 Ebenda, S. 1583 (1596 f.).

verarbeiteten Daten ableiten lassen könnte.[340] Ist diese Wahrscheinlichkeit hoch genug, kann davon ausgegangen werden, dass es sich bei den Daten um besondere Kategorien von personenbezogenen Daten handelt.

Für die Bevorzugung der kontextabhängigen Bestimmung könnte die englische Formulierung der DSGVO sprechen. Beim Abgleich zwischen der deutsch- und englischsprachigen Version der DSGVO fällt nämlich auf, dass in der Formulierung des Art. 9 Abs. 1 DSGVO ein kleiner, aber wesentlicher Unterschied besteht. Während in der deutschen Fassung von „biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person" die Rede ist, steht in der englischen Fassung „biometric data for the purpose of uniquely identifying a natural person". Damit findet im Englischen in Bezug auf biometrische Daten eine explizite sprachliche Verknüpfung mit einem Zweck statt. Für die anderen genannten Beispiele liegt keine solche Verknüpfung mit einem bestimmten Verarbeitungszweck vor, weswegen davon ausgegangen wird, dass diese kontextabhängig als besondere Kategorien von personenbezogenen Daten bestimmt werden müssen.[341] Eine ähnliche Bevorzugung der kontextabhängigen Bestimmung scheint sich nach einiger Auffassung auch in der ehemaligen EU-Datenschutz-Richtlinie zu finden.[342]

b. Probleme mit der kontextabhängigen Bestimmung

Eine kontextabhängige Bestimmung von besonderen Kategorien von personenbezogenen Daten führt auf Seiten der Verantwortlichen allerdings wahrscheinlich zu Unklarheit. Zwar können maßgebliche Kriterien für die Bewertung des Gesamtzusammenhanges festgelegt werden, allerdings lassen diese noch etlichen Interpretations- und Gewichtungsspielraum zu. Nach dieser Herangehensweise könnte also das gleiche personenbezogene Datum in einem Fall als besondere Kategorie von personenbezogenen Daten eingestuft werden und in einem anderen Fall wiederum nicht.[343] Ebenso könnte das gleiche personenbezogene Datum im gleichen Verarbeitungskontext sowohl als sensitiv als auch als nicht-sensitiv eingestuft werden,

340 *Albers/Veit* (2020), Art. 9 Rn. 29 ff.; *Schiff* (2018), Art. 9 Rn. 13; *Weichert* (2020), Art. 9 Rn. 24; *Malgieri/Comandé,* Information & Communications Technology Law 2017, S. 229 (239).

341 *Petri* (2019), Art. 9 Rn. 12; *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1594).

342 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1592 f.).

343 *Frenzel* (2021), Art. 9 Rn. 6.

je nachdem, wie jeweilige Bewertungskriterien interpretiert und gewichtet werden. Dies öffnet die Tür für subjektiv vorteilhafte und ggf. auch böswillige Bewertungen des Gesamtzusammenhangs durch nicht vertrauenswürdige Verantwortliche. Die Etablierung von objektiven kontextabhängigen Bestimmungen wäre somit von langwierigen und aufwändigen Rechtsverfahren und Urteilssprüchen abhängig. Hinzu kommt, dass sich der Status eines Datums bereits bei Änderung eines Aspekts in der Bewertung des Gesamtzusammenhangs ändern kann, womit ggf. eine hohe Volatilität bei der Bestimmung von besonderen Kategorien von personenbezogenen Daten entstehen könnte.

Grundsätzlich ist allerdings davon auszugehen, dass eine kontextabhängige Bestimmung dazu führen würde, dass die Definition von besonderen Kategorien von personenbezogenen Daten enorm auswuchern würde.[344] Denn die Wahrscheinlichkeit, dass sich eine sensitive Information bei dem jeweiligen Verarbeitungskontext aus den verarbeiteten Daten ableiten lassen könnte, ist bereits sehr hoch und wird in Zukunft aufgrund von technologischer Entwicklung wahrscheinlich noch höher werden. Mit zunehmender Rechenkraft, Verbreitung von Data-Mining und steigender Datenverknüpfungsmöglichkeit, wird es auch wahrscheinlicher, dass aus grundsätzlich nicht-sensitiven Daten kontextabhängig häufiger sensitive Daten werden, womit eine enorme Menge an Daten unter Art. 9 Abs. 1 DSGVO gezählt werden könnten.[345]

Dies führt wiederum zu dem Problem, dass ohnehin schon komplexe Datenverarbeitungstätigkeiten für betroffene Personen noch unverständlicher werden würden. Wenn zunehmend scheinbar nicht-sensitive Daten durch Verantwortliche kontextabhängig als besondere Kategorien von personenbezogenen Daten eingestuft werden, könnte dies zu mehr Unsicherheit auf Seiten der Betroffenen führen. Da diesen der Verarbeitungskontext meist nicht ausreichend bekannt sein wird, ist die Bestimmung von sensitiven Informationen kaum nachvollziehbar. Auch wenn der Gesamtzusammenhang der Verarbeitung komplett offengelegt werden würde, würden damit nur noch mehr Informationen entstehen, die für die gewöhnlich betroffene Person zu umfangreich und kaum verständlich sein dürften. Hinzu kommt, dass die wahrscheinliche Volatilität bei der Bestimmung von sensitiven Informationen auch die Abschätzung der Folgen einer Datenver-

344 *Poullet/Dinant,* Report On The Application Of Data Protection Principles To The Worldwide Telecommunication Networks, S. 43; *Schiff* (2018), Art. 9 Rn. 14.

345 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1596 f. und 1599); *Frenzel* (2021), Art. 9 Rn. 8.

arbeitung seitens Betroffener unnötig erschweren würden. In der Bilanz würde die Intransparenz in Bezug auf entsprechende Datenverarbeitungen demnach wahrscheinlich steigen.

c. Zweckabhängige Bestimmung

Im Gegensatz zur kontextabhängigen Bestimmung wird bei einer zweckabhängigen Bestimmung auf die Auswertungsabsicht des Verantwortlichen abgestellt.[346] Der Status als besondere Kategorien von personenbezogenen Daten definiert sich demnach über die konkrete Verarbeitung bzw. über den zugrundeliegenden Verarbeitungszweck.[347] Wenn bspw. Likes auf einer Social Media-Plattform nur zu dem Zweck verarbeitet werden, um Zustimmung zu Beiträgen zu ermöglichen, liegen keine sensitiven Informationen vor. Sobald allerdings Likes verarbeitet werden, um Persönlichkeitsprofile zu erstellen, in denen dann politische Einstellung, Sexualität und Weiteres enthalten sind, ist der Anwendungsbereich zweckabhängig eröffnet.

Für die Bevorzugung der zweckabhängigen Bestimmung spricht, dass diese Vorgehensweise mit einem vergleichsweise geringen administrativen Aufwand für die Aufsichtsbehörden einhergehen würde und wahrscheinlich auch weniger triviale Fälle vor Gericht verhandelt werden müssten.[348] Hinzu kommt, dass die zweckabhängige Bestimmung im Vergleich zur kontextabhängigen Bestimmung auf Seiten der Verantwortlichen für mehr Klarheit in der Datenschutz-Praxis sorgen würde. Ebenso würde die Datenverarbeitung für Betroffene besser verständlich und transparenter sein, da sich der Status ihres personenbezogenen Datums lediglich über das Merkmal des Verarbeitungszwecks/der Verarbeitungsabsicht bestimmt.

346 *Schulz* (2018), Art. 9 Rn. 13; *Frenzel* (2021), Art. 9 Rn. 9; *Schneider/Schindler,* ZD 2018, S. 463 (467).

347 *Poullet/Dinant,* Report On The Application Of Data Protection Principles To The Worldwide Telecommunication Networks, S. 43.

348 *Wong,* Journal of International Commercial Law and Technology 2007, S. 9 (12).

d. Probleme mit der zweckabhängigen Bestimmung

Auch bei diesem Vorgehen besteht allerdings das Problem im subjektiven Spielraum bei der Festlegung von Verarbeitungszwecken.[349] So kann ein Verantwortlicher bspw. bewusst eine grobe Definition des Verarbeitungszwecks wählen, woraus nicht direkt hervorgeht, dass damit eine Absicht besteht, sensitive Informationen zu erheben oder zu erzeugen. So deutet der Zweck, ein Nutzerprofil zu erstellen, nicht zwangsläufig auf besondere Kategorien von personenbezogenen Daten hin. Allerdings schließt dieser die Verarbeitung solcher Informationen auch nicht aus. Zentral steht dabei die Sorge, dass Verantwortliche diesen Spielraum zu ihrem Vorteil ausnutzen oder gar falsche Verarbeitungszwecke angeben, welche nur schwer widerlegt werden könnten.[350]

Ebenso könnte die zweckabhängige Bestimmung dazu führen, dass mit Daten, die aufgrund ihres (potenziellen) Informationsgehaltes eigentlich als sensitiv eingestuft werden müssten, aber aufgrund des gewählten, eher trivialen Zwecks wie gewöhnliche Daten behandelt werden, häufiger nachlässiger umgegangen wird. Diese nachlässige Verarbeitung könnte dann das Risiko von Datenschutzvorfällen und Missbrauch seitens Dritter erhöhen.[351]

Ergänzend besteht auch noch die Problematik, dass die DSGVO in Art. 6 Abs.4 eine Zweckänderung ermöglicht. Allerdings ist umstritten, inwiefern sich dies auch bei Daten, die unter Art. 9 Abs. 1 DSGVO fallen, anwenden lässt.[352] Nichtsdestotrotz besteht die Sorge, dass die Möglichkeit einer Zweckänderung sowie die Ausnahmen der Zweckbindung gemäß Art. 5 Abs. 1 lit. b DSGVO bei der Verarbeitung von besonderen Kategorien von personenbezogenen Daten dazu führen könnten, dass nachträgliche Anpassungen des Verarbeitungszwecks den Status eines Datums jederzeit ändern könnten, womit die Planung der Verarbeitung seitens des Verantwortlichen sowie die Abschätzung der Verarbeitungsauswirkung für Betroffene verkompliziert wird.[353]

---

349 *Frenzel* (2021), Art. 9 Rn. 9; *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1595).

350 *Albers/Veit* (2020), Art. 9 Rn. 30; *Petri* (2019), Art. 9 Rn. 12; *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1594 f.).

351 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1595).

352 Pro: *Schulz* (2018), Art. 9 Rn. 7; Contra: *Schiff* (2018), Art. 9 Rn. 11.

353 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1595 f.).

e. Mögliche Kombination beider Bestimmungsansätze

Beide Vorgehensweisen haben den Nachteil, dass die Bestimmung von sensitiven Informationen vor allem subjektiv ist und kaum an objektiven Kriterien festgemacht werden kann. Hinzu kommt, dass die kontextabhängige Bestimmung von besonderen Kategorien von personenbezogenen Daten ein sehr weites Verständnis von Sensitivität zur Folge hätte und insg. wahrscheinlich für weniger Transparenz sorgen würde. Die zweckabhängige Bestimmung könnte ergänzend wiederum dazu führen, dass mit eigentlich sensitiven Daten unvorsichtiger umgegangen wird, womit das Risiko für Datenschutzvorfälle steigen könnte. Ebenso könnten Zweckänderungen eine Herausforderung für diese Vorgehensweise bedeuten.

Um die Problematik aufzulösen, wird häufig eine Kombination beider Bestimmungsansätze als sinnvoll erachtet.[354] Zusammengefasst soll unter Berücksichtigung des Verarbeitungskontextes, allerdings mit dem Fokus auf der Auswertungsabsicht des Verantwortlichen[355] und in Abhängigkeit zum durchschnittlichen Empfängerhorizont[356] festgestellt werden, ob besondere Kategorien von personenbezogenen Daten vorliegen. Damit soll sichergestellt werden, dass der Anwendungsbereich des Art. 9 DSGVO nicht unnötig aufgebläht wird, aber nichtsdestotrotz ein ausreichender Schutz für Betroffene bestehen bleibt. Ebenso wird mit dem teilweise objektivierbaren, durchschnittlichen Empfängerhorizont ein Mechanismus ergänzt, der die ansonsten mehrheitlich subjektive Bestimmung eindämmen könnte.

f. Probleme mit der Kombination beider Bestimmungsansätze

Fraglich ist allerdings, ob eine Kombination beider Bestimmungsansätze praktikabler ist. Auch hier bleibt die Subjektivität in der Einschätzung ein zentrales Problem. Ebenso bräuchte es dafür zunächst ein festgelegtes einheitliches Vorgehen, damit eine allgemeine Konsistenz bei der Bestimmung von sensitiven Daten gewährleistet wird. Da von einem zeitnahen diesbezüglichen Konsens nicht ausgegangen werden kann, würde wahr-

354 *Spindler/Dalby* (2019), Art. 9 DSGVO Rn. 4; *Mester* (2019), Art. 9 Rn. 6; *Weichert* (2020), Art. 9 Rn. 22 f.; *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1609 f.); *McCullagh,* Journal of International Commercial Law and Technology 2007, S. 190 (200).

355 *Frenzel* (2021), Art. 9 Rn. 9; *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1609 f.)

356 *Weichert* (2020), Art. 9 Rn. 22 f.

scheinlich die gleiche Verwirrung in der Datenschutz-Praxis und Fachwelt bestehen bleiben, wie derzeit schon. Dies macht es somit fraglich, ob eine Kombination beider Ansätze tatsächlich zu mehr Klarheit führen würde. Für gewöhnliche Verantwortliche bleibt der durchschnittliche Empfängerhorizont z.B. immer noch Auslegungssache und für Betroffene wird damit ebenso wenig für mehr Transparenz bei der Verarbeitung ihrer Daten gesorgt.

g. Vorgehen in der Praxis: Beispiel Facebook

Wie genau die Bestimmung von besonderen Kategorien von personenbezogenen Daten stattzufinden hat, ist noch nicht abschließend geklärt. Weder in der relevanten Literatur findet sich ein Konsens, noch gibt es richterliche Klarstellungen zu dieser Frage. Für betroffene Personen ist diese fehlende Eindeutigkeit allerdings wenig relevant. Viel relevanter ist für Betroffene, wie mit sensitiven Daten in der Datenschutz-Praxis tatsächlich umgegangen wird. Folgendes Beispiel soll somit die Problematik zwischen kontext- oder zweckabhängiger Bestimmung von besonderen Kategorien von personenbezogenen Daten verdeutlichen und zeigen, welcher Weg in der Praxis häufig gewählt wird.

Laut Facebooks Datenschutzerklärung dient die Einwilligung gemäß Art. 9 Abs. 2 lit. a DSGVO als Rechtsgrundlage „für die Verarbeitung von Daten mit besonderem Schutz" worunter alle Datenarten nach Art. 9 Abs. 1 DSGVO fallen.[357] Zusammengefasst verarbeitet Facebook besondere Kategorien von personenbezogenen Daten auf Grundlage einer Einwilligung, um vom Nutzer geteilte, sensitive Inhalte mit den vom Nutzer ausgewählten Personen teilen zu können sowie, um angezeigte Inhalte für den Nutzer zu personalisieren. Was es konkret bedeutet, Inhalte zu personalisieren, wird nicht genauer ausgeführt. Es ist davon auszugehen, dass dies darauf abzielt, im persönlichen Feed solche Inhalte anzuzeigen, die dem Nutzer aufgrund seines bisherigen Nutzungsverhaltens am wahrscheinlichsten gefallen werden.

Das bisherige Nutzungsverhalten bzw. die kumulierten Tätigkeiten der betroffenen Person auf Social-Media Plattformen können allerdings auch

357 Abgerufen unter https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 (abgerufen 4.1.2025).

genutzt werden, um Wahlprognosen und Scores zu ermitteln.[358] Der Cambridge Analytica-Fall hat gezeigt, dass solche Auswertungen von Facebook-Nutzern verwendet werden können, um personen- und interessensspezifische Inhalte anzuzeigen, die ggf. Auswirkung auf das Wahlverhalten haben könnten.[359] Somit ist es nicht verwunderlich, dass bereits etliche politische Akteure personen- und interessensspezifische Wahlwerbung über Facebook haben schalten lassen.[360] Eine Datenauswertung des *ZDF Magazin Royal* zum Bundestagswahlkampf 2021 fand heraus, welche Targeting-Kriterien (z.B. Interesse, Standort, Job, Verhalten) von welchen Parteien genutzt wurden, um jene Menschen zu erreichen, deren Interessen etc. wahrscheinlich am ehesten mit der jeweiligen Parteiposition übereinstimmen könnten.[361] So ließ bspw. die Partei Bündnis 90/Die Grünen ihre Wahlwerbung an Menschen ausliefern, die sich für Nachhaltigkeit, Umweltschutz und Klimaschutz interessierten.[362] Eine weitere Untersuchung aus 2017 stellte fest, dass es sogar möglich war, explizit Anzeigen an Antisemiten auszuspielen.[363] Eine andere Studie kam zu dem Schluss, dass Facebook 67 % aller Nutzer mit Werbepräferenzen versieht, die potentiell sensitiv sind und unter Art. 9 Abs. 1 DSGVO subsumiert werden könnten.[364]

Gemäß der kontextabhängigen Bestimmung von besonderen Kategorien von personenbezogenen Daten stellt Facebook bei der Schaltung von Werbeanzeigen demnach eindeutig personenbezogene Daten zur Verfügung, aus denen mit hinreichender Wahrscheinlichkeit u.a. die politische Meinung hervorgehen könnte. Demnach bedürfte es für ebenjene Datenverarbeitung eine Rechtsgrundlage aus Art. 9 Abs. 2 DSGVO. Wie der Datenschutzerklärung von Facebook zu entnehmen ist, ist eine solche Verarbeitung von besonderen Kategorien von personenbezogenen Daten zu Marke-

358 *Christl,* Aus Politik und Zeitgeschichte 2019, S. 42 (46 ff.).
359 *Chester/Montgomery,* Internet Policy Review 2017, S. 1 (7); *Christl,* Aus Politik und Zeitgeschichte 2019, S. 42 (46 ff.).
360 *Wong,* It might work too well: the dark art of political advertising online, v. 19.3.2018, https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy (abgerufen 30.4.2022).
361 Abrufbar unter: https://targetleaks.de/netzwerkdiagramme (abgerufen am 1.5.2022).
362 Ebenda.
363 *Angwin/Varner/Tobin:* Facebook Enabled Advertisers to Reach „Jew Haters", v. 14.9.2017, https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters (aufgerufen 30.4.2022).
364 *Cabañasn et al.,* Communications of the ACM 2021, S. 62 (66).

tingzwecken allerdings nicht von der Einwilligung der betroffenen Person erfasst.[365]

Gemäß der zweckabhängigen Bestimmung von besonderen Kategorien von personenbezogenen Daten könnte wiederum argumentiert werden, dass Facebook die Daten nicht explizit mit dem Zweck verarbeitet, um Wahlwerbung anzuzeigen, die der politischen Einstellung der jeweiligen Person entspricht, sondern lediglich, um detaillierte Targeting-Kriterien für Werbekunden bereitzustellen. Gemäß dieser Herangehensweise würden vielmehr erst die politischen Parteien eine Datenverarbeitung erzeugen, die unter Art. 9 Abs. 1 DSGVO zu subsumieren wäre. Schließlich besteht erst dann der Zweck der Verarbeitung darin, personenspezifische Wahlwerbung anzuzeigen. Die Bereitstellung der Targeting-Kriterien seitens Facebook bedürfe demnach keiner speziellen Rechtsgrundlage aus Art. 9 Abs. 2 DSGVO. Diese würde erst notwendig, wenn die Kriterien explizit zu einem Zweck verarbeitet werden, aus dem dann bspw. die politische Meinung hervorgehen könnte.

Aus der Datenschutzerklärung von Facebook geht hervor, dass das Unternehmen eine solche Datenverarbeitung zu Marketingzwecken scheinbar zu keiner Zeit unter Art. 9 Abs. 1 DSGVO fasst. Zwar wird für die Personalisierung von Werbung noch eine gesonderte Einwilligung eingeholt, welche dann allerdings nicht mehr besondere Kategorien von personenbezogenen Daten umfasst.[366] Vielmehr beruft sich die Plattform prinzipiell auf das berechtigte Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO, welches für Daten i.S.v. Art. 9 Abs. 1 DSGVO nicht in Frage kommt, um Messungen und Analysen für Werbekunden durchzuführen und um dementsprechend Berichte für die Kunden bereitzustellen.[367] Was genau unter Analysen und Berichte zu verstehen ist, wird nicht weiter ausgeführt. Es ist aber davon auszugehen, dass damit Rückmeldungen seitens Facebook bzgl. der Wirksamkeit von Werbeanzeigen gemeint sind. Aus solchen Rückmeldungen geht dann hervor, welche Zielgruppe durch die geschaltete Anzeige zur Interaktion angeregt wurde. Mithilfe dieser Rückmeldung können politische Parteien bspw. abgleichen, ob die gewählten Targeting-Kriterien auch tatsächlich die Menschen erreichen, für die solche Anzeigen am wahrscheinlichsten

365 Abgerufen unter https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 (abgerufen 5.1.2025).

366 Abgerufen unter https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 (abgerufen 4.1.2025).

367 Abgerufen unter https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 (abgerufen 4.1.2025).

interessant wären. Demnach könnten die Analysen und Berichte für Werbekunden auch sensitive Informationen über Betroffene enthalten.

Am beispielhaften Fall von Wahlwerbung auf Facebook konnte dargelegt werden, dass sich solche Datenverarbeitungen oftmals im juristischen Graubereich befinden. Kontextabhängig dürften etwaige Verarbeitungen von personenbezogenen Daten dazu führen, dass der Anwendungsbereich von Art. 9 Abs. 1 DSGVO prinzipiell eröffnet ist. Zweckabhängig würde das Abstellen auf die Auswertungsabsicht dazu führen, dass nicht die allgemeine Datenverarbeitung unter Art. 9 Abs. 1 DSGVO fällt, sondern lediglich sensitive Teilaspekte der Verarbeitung. Gemeinsam haben beide Vorgehensweisen, dass diese für Verantwortliche sehr aufwändig und auch hinderlich in der Verfolgung der Geschäftsziele sind. Demnach hat sich in der Praxis vielmehr durchgesetzt, dass die offensichtlichen Fälle (beim Beispiel Facebook das Teilen von offensichtlichen Gesundheitsdaten o.ä.) meist gemäß Art. 9 Abs. 1 DSGVO gehandhabt werden, wohingegen die Graubereiche oftmals zweckabhängig vorteilhaft ausgelegt werden.

3. Wesensdaten als besondere Kategorie von personenbezogenen Daten

a. Die Besonderheit von Wesensdaten

Das Besondere an Wesensdaten ist, dass diesen nicht ein abschließender Aussagegehalt zugeschrieben werden kann, sodass auch eine eindeutige Zuordnung zu einer bestimmten Datenkategorie nicht möglich ist. Im Vergleich z.B. zu genetischen Daten, wird diese Besonderheit schnell klar. Genetische Daten lassen sich in ihrem Aussagegehalt klar definieren und von anderen Daten abgrenzen. Aus der Analyse aus Kapitel F.I.1.e geht hervor, dass der Aussagegehalt von genetischen Daten auf die genetischen Eigenschaften einer Person beschränkt sind, die bspw. über eine Chromosomen-, DNS- und/oder RNA-Analyse ermittelt werden können. Damit können genetische Daten eindeutig von anderen Datenkategorien unterschieden werden. Eine DNS-Probe ist somit immer in die Datenkategorie „genetische Daten" einzuordnen. Zwar sind noch weitere Unterkategorisierungen möglich, z.B. wenn die Probe Aussagen über die rassische oder ethnische Herkunft einer Person macht, doch ändert dies nichts an der Tatsache, dass eine DNS-Probe in erster Linie ein genetisches Datum ist, welches alleinstehend von Daten zur rassischen oder ethnischen Herkunft abgegrenzt werden kann. Im Gegensatz zu genetischen Daten können Wesensdaten

aber nicht ohne Weiteres eindeutig abgegrenzt werden. Demnach liegt bei Wesensdaten keine grundsätzliche intrinsische Sensitivität vor, was die Einstufung als besondere Kategorie von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO erschwert.

Der Definition aus Kapitel E.IV folgend, liegen Wesensdaten dann vor, wenn anhand eines neurologischen (Roh-)Datensatzes Auswertungen vorgenommen werden können, die mithilfe von technologischer Erweiterung des menschlichen Gehirns und zentralen Nervensystems Outputs generieren können und/oder fallabhängige Aussagen über äußere und/oder innere Wesensmerkmale machen können, die eindeutige Rückschlüsse auf das individuelle Wesen einer Person zulassen. Wie in Kapitel B.I u. II und D.I dargelegt, können diese Outputs und Aussagen viele Formen annehmen. Wesensdaten können somit Daten sein, die Rückschlüsse auf die rassische und ethnische Herkunft zulassen,[368] aus denen die politische Meinung hervorgeht,[369] die teilweise die religiöse oder weltanschauliche Überzeugung offenbaren,[370] die Aussagen über die sexuelle Orientierung und das Sexualleben machen,[371] die als Gesundheitsdaten definiert werden können[372] und die als biometrische Daten die eindeutige Identifizierung einer natürlichen Person ermöglichen.[373]

b. Einstufung von Wesensdaten gemäß der kontextabhängigen Bestimmung

Gemäß der kontextabhängigen Bestimmung dürften Wesensdaten somit in den meisten Fällen als sensitive Daten gemäß Art. 9 Abs. 1 DSGVO einzustufen sein. Besonders in Anbetracht der Technik, die bei der Datenverarbeitung Anwendung findet, und des (zukünftigen) Auswertungspotentials

368 *Tang et al.,* NeuroImage 2010, S. 33 (36 ff.).
369 *Schreiber et al.,* PLOS ONE 2013, S. 1 (2f.); *Vecchiato et al.,* 31st Annual International Conference of the IEEE EMBS 2009, S. 57 (59f.).
370 *Knutson et al.,* Human Brain Mapping 2007, S. 915 (927).
371 *Safron et al.,* Scientific Reports 2018 (8), S. 1 (7 ff.); *Hammilton/Meston,* Archive of Sexual Behavior 2017, S. 2289 (2294 f.).
372 *Bansal/Mahajan,* EEG-Based Brain-Computer Interfaces: Cognitive Analysis and Control Applications, 2019, S. 61; *Mattia/Molinari,* in: Grübler/Hildt, Brain-Computer Interfaces in their ethical, social and cultural contexts, 2014, S. 49 (50f); *Sebastián-Romagosa et al.,* Frontiers of Neuroscience 2020, S. 1 (5).
373 *Landau/Puzis/Nissim,* AMC Computing Surveys 2020, S. 1 (12 ff.); *Qui et al.,* ACM Computing Surveys 2019, S. 1 (3 ff.).

dürfte der Gesamtzusammenhang der Verarbeitung häufig für das Vorliegen von sensitiven Daten sprechen.[374]

c. Einstufung von Wesensdaten gemäß der zweckabhängigen Bestimmung

Bei der zweckabhängigen Bestimmung ist die Einstufung allerdings nicht eindeutig. Wesensdaten können laut dieser Betrachtungsweise zwar sensitive Daten i.S.v. Art. 9 Abs. 1 DSGVO sein, allerdings liegt die Betonung dabei auf „können". Denn nur weil Wesensdaten vorliegen, heißt das nicht automatisch, dass diese gemäß der zweckabhängigen Bestimmung auch prinzipiell als sensitive Daten einzustufen sind. Wesensdaten können demnach also besondere Kategorien von personenbezogenen Daten i.S.v. Art. 9 Abs. 1 DSGVO sein, müssen es aber nicht. Bei einer zweckabhängigen Bestimmung würden Wesensdaten, die lediglich für den Zweck verarbeitet werden, einen Roboter per Gedanke zu steuern, schließlich nicht unter Art. 9 Abs.1 DSGVO zu subsumieren sein. Werden diese dahingegen zum Zweck der Diagnose von psychischen Krankheiten verwendet, liegen eindeutig Gesundheitsdaten vor, womit der Status als sensitives personenbezogenes Datum gegeben wäre. Demnach fallen diese gemäß der zweckabhängigen Bestimmung nicht kategorisch unter den besonderen Schutz des Art. 9 DSGVO, sondern können nur einzelfallbezogen und abhängig vom konkreten Verarbeitungszweck als besondere Kategorien von personenbezogenen Daten eingestuft werden.[375]

d. Wahrscheinlicher Umgang mit Wesensdaten in der Praxis

Wie dargelegt werden konnte, ist die Einordnung von Wesensdaten in den Reglungsbereich von Art. 9 Abs. 1 DSGVO nicht eindeutig. Für die betroffenen Personen wird diesbezüglich darum vor allem relevant sein, wie in der Datenschutz-Praxis mit ihren Wesensdaten umgegangen wird. Wie in Kapitel H.I.2.f ausgeführt wurde, hat sich in der Praxis ein Vorgehen

374 Anderer Meinung: *Ienca/Malgieri,* Journal of Law and the Biosciences 2022, S. 1 (10). - gehen zwar davon aus, dass eine kontextabhängige Bestimmung vorgenommen werden muss, kommen aber zu dem Schluss, dass eine konzeptionelle und normative Lücke besteht, womit neurologische Daten nicht unter Art. 9 Abs. 1 DSGVO fallen würden.

375 Ähnlicher Meinung: *Rainey et al.,* Journal of Law and the Biosciences 2020, S. 1 (13 ff.).

durchgesetzt, wobei die offensichtlichen Fälle (beim Beispiel Facebook das Teilen von offensichtlichen Gesundheitsdaten o.Ä.) meist gemäß Art. 9 Abs. 1 DSGVO gehandhabt werden, wohingegen die Graubereiche oftmals zweckabhängig vorteilhaft ausgelegt werden könnten.

Für die zukünftige Verarbeitung von Wesensdaten könnte dies bedeuten, dass lediglich die eindeutigen Verarbeitungssituationen, bei denen bspw. eine Diagnose von psychischen Erkrankungen vorgenommen wird, unter den besonderen Schutz von Art. 9 Abs. 1 DSGVO fallen dürften, wodurch kein kategorischer Schutz für Wesensdaten entstehen würde.

Fraglich ist allerdings, ob eine solche vorwiegend zweckgebundene Einstufung dem Informationsschöpfungspotential von Wesensdaten und der daraus entstehenden Gefahr für die Handlungsfreiheit von Smart Human gerecht wird - besonders wenn man bedenkt, dass dann das berechtigte Interesse aus Art. 6 Abs. 1 lit. f DSGVO nicht als legitime Rechtsgrundlage ausgeschlossen ist.

Nachfolgend sollen darum die möglichen Rechtsgrundlagen und somit auch das berechtige Interesse genauer betrachtet und auf die Verarbeitung von Wesensdaten angewandt werden.

II. Rechtfertigungsgründe – Analyse Art. 6 Abs. 1 DSGVO

Eine Datenverarbeitung ist nur dann rechtmäßig, wenn mindestens eine Bedingung aus Art. 6 Abs.1 UAbs. 1 DSGVO erfüllt ist. Dabei ist es dem Verantwortlichen überlassen, welcher konkrete Erlaubnistatbestand herangezogen wird, um die Datenverarbeitung im Einklang mit dem Gesetz zu gestalten.[376] Im Nachfolgenden werden die Rechtsgrundlagen aus Art. 6 Abs. 1 UAbs. 1 DSGVO analysiert, die für BCI am relevantesten sind und zwar die Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO) und das berechtigte Interesse (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO). Auf Grundlage der Analyseergebnisse soll dann überprüft werden, ob die bestehenden Erlaubnistatbestände die Datenverarbeitung durch BCI sinnvoll reglementieren können.

376 *Buchner/Petri* (2020), Art. 6 Rn. 22.

1. Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO: Einwilligung

Die Einwilligung spielt eine zentrale Rolle in Bezug auf die informationelle Selbstbestimmung, da sie der betroffenen Person die Möglichkeit gibt, selbstständig darüber zu entscheiden, was genau mit ihren personenbezogenen Daten passiert.[377] Aus diesem Grund gelten auch strenge Wirksamkeitsvoraussetzungen für die Einwilligung, die neben Art. 6 Abs. 1 UAbs. 1 lit. a noch in Art. 4 Nr. 11, Art. 7, Art. 8 und Art. 9 Abs. 2 lit. a DSGVO konkretisiert werden. Gemäß der Legaldefinition aus Art. 4 Nr. 11 DSGVO ist eine Einwilligung „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist." Art. 7 und 8 DSGVO ergänzt diese Definition um explizite Bedingungen, die eine Einwilligung erfüllen muss, um rechtskräftig zu sein, auch in Bezug auf die Einwilligung eines Kindes. Art. 9 Abs. 2 lit. a DSGVO rundet den Reglungsbereich ab und konkretisiert den Einsatz von Einwilligungen im Kontext von besonderen Kategorien von personenbezogenen Daten. Aus diesen formgebenden Artikeln lassen sich folgende Wirksamkeitsvoraussetzungen ableiten: Freiwilligkeit, Transparenz, Zweckbindung, Eindeutigkeit/Formerfordernis.[378]

Freiwilligkeit ist laut ErwG. 42 S. 5 dann gegeben, wenn die betroffene Person keine negativen Konsequenzen fürchten muss, wenn diese ihre Einwilligung nicht gibt oder sie zurückzieht. Betroffene sollen vielmehr eine tatsächliche Wahl haben. Demnach kann eine rechtmäßige Einwilligung nicht erzwungen oder forciert werden,[379] sodass gemäß ErwG. 43 eine besondere Berücksichtigung des Machtgefälles zwischen betroffener Person und Verantwortlichen notwendig ist. Unterstrichen wird dies durch Art. 7 Abs. 4 DSGVO, welcher es verbietet, die Erfüllung eines Vertrags mit einer Einwilligung zu einer Datenverarbeitung zu koppeln. Der Gesetzgeber macht damit unmissverständlich deutlich, dass Freiwilligkeit eine zentrale Voraussetzung für die Wirksamkeit der Einwilligung ist.[380] Um diese Freiwilligkeit vollumfänglich zu gewährleisten, steht es der betroffenen Person gemäß Art. 7 Abs. 3 DSGVO jederzeit zu, die Einwilligung zu widerrufen.

377 *Buchner/Petri* (2020), Art. 6 Rn. 17; *Taeger* (2019), Art. 6 Rn. 23.
378 *Taeger* (2019), Art. 6 Rn. 29 ff.; Heberlein (2018), Art. 6 Rn. 7 ff.
379 *Taeger* (2019), Art. 6 Rn. 29.
380 *Krohm*, ZD 2016, S. 368 (373).

Notwendige Voraussetzung für eine tatsächliche Wahl ist wiederum die vollkommende Transparenz der geplanten Verarbeitung, sodass die betroffene Person nachvollziehen kann, wer für die Verarbeitung verantwortlich ist und was genau mit ihren personenbezogenen Daten passieren wird.[381] Nur so kann gemäß Art. 4 Nr. 11 DSGVO eine Einwilligung in informierter Weise abgegeben werden. Der Umfang der für die Transparenz notwendigen Informationen wird durch Art. 12 – 14 DSGVO festgelegt.[382] Art. 7 Abs. 3 S. 3 DSGVO ergänzt diesen Umfang um die notwendige Mitteilung über das Recht auf Widerruf der Einwilligung. Die notwendigen Angaben sind dabei laut Art. 12 Abs. 1 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Eine Formerfordernis besteht für diese Informationen nicht, doch da der Verantwortliche im Zweifel nachweisen können muss, dass eine rechtmäßige Einwilligung vorliegt, ist die Schriftform zu empfehlen.[383] Die vorgelagerte Information der betroffenen Person ist neben der Freiwilligkeit somit ausschlaggebend für eine rechtskräftige Einwilligung.[384]

Ergänzend ist ebenso eine Zweckbindung bei einer Einwilligung notwendig, damit diese als valide Rechtsgrundlage für die Datenverarbeitung fungieren kann. Laut Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO kann die Einwilligung für „einen oder mehrere bestimmte Zwecke" abgegeben werden. Daraus geht hervor, dass allgemeine Einwilligungen zu undefinierten Zwecken nicht rechtmäßig sind.[385] Des Weiteren sind damit zwar umfangreiche Einwilligungen möglich, die sich auf eine Vielzahl von Zwecken beziehen, allerdings ist eine Weiterverarbeitung der Daten zu abweichenden Zwecken auf Grundlage der Einwilligung ausgeschlossen.[386] Durch die Zweckbindung hat die Einwilligung keine konkrete zeitliche Beschränkung, aber wird in dem Moment ungültig, in dem der Zweck erreicht wurde oder verfallen ist.[387] Damit wird der Zweckbindungsgrundsatz aus Art. 5 Abs. 1 lit. b DSGVO in Bezug auf die Einwilligung explizit aufgegriffen.[388]

Für die Einwilligung wird gesetzlich keine bestimmte Form vorgegeben. Allerdings verlangt Art. 4 Nr. 11 DSGVO eine „unmissverständlich abge-

381 *Heberlein* (2018), Art. 6 Rn. 8.
382 *Heberlein* (2018), Art. 6 Rn. 8; *Taeger* (2019), Art. 6 Rn. 33 f.
383 *Taeger* (2019), Art. 6 Rn. 34.
384 *Heberlein* (2018), Art. 6 Rn. 8.
385 Ebenda, Rn. 9.
386 *Taeger* (2019), Art. 6 Rn. 38.
387 *Schulz* (2018), Art. 6 Rn. 26.
388 *Heberlein* (2018), Art. 6 Rn. 9.

gebene Willensbekundung in Form einer […] eindeutigen bestätigenden Handlung". Dies setzt ein explizites Tätigwerden der betroffenen Person voraus. Laut ErwG. 32 liegt ein solches Tätigwerden z.B. vor, wenn die betroffene Person aktiv ein Kästchen auf einer Internetseite auswählt oder bei Diensten der Informationsgesellschaft technische Einstellungen anpasst, während in Stillschweigen oder Untätigkeit keine eindeutig bestätigende Handlung zu sehen ist. Schlüssiges Verhalten ist somit nicht auszuschließen und kann als wirksame konkludente Einwilligung gezählt werden.[389]

In Bezug auf besondere Kategorien von personenbezogenen Daten, werden die Wirksamkeitsvoraussetzungen durch Art. 9 Abs. 2 lit. a DSGVO um das Merkmal der Ausdrücklichkeit ergänzt. Die Einwilligung muss sich demnach ausdrücklich auf die Verarbeitung von besonderen Kategorien von personenbezogenen Daten beziehen und die konkludente Einwilligung wird für alle Daten, die unter Art. 9 Abs. 1 DSGVO fallen, ausgeschlossen.[390] Dies erfordert, dass die betroffene Person genaustens über die geplante Verarbeitung inkl. der besonderen Daten informiert wird, da nur so eine eindeutige und zweifelsfreie Einwilligung zustande kommen kann.[391] Entsprechend gelten an eine Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO noch höhere Ansprüche bzgl. Genauigkeit und Transparenz.[392]

2. Das Problem mit der Einwilligung als Rechtsgrundlage

Die Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO findet als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten in vielen Konstellationen Anwendung. Allerdings stellt sich die grundsätzliche Frage, ob der datenschutzrechtliche Einwilligungsmechanismus im Allgemeinen überhaupt die selbstauferlegten Voraussetzungen erfüllen kann. Etliche Umfragen und Auswertungen haben herausgefunden, dass Rechtsdokumenten wie AGBs oder Datenschutzerklärungen zugestimmt wird, obwohl die meisten Menschen diese nicht lesen.[393] Die Anzahl der Menschen, die in Europa Datenschutzerklärungen im Internet vollständig lesen,

389 *Klement* (2019), Art. 7 Rn. 35.
390 *Kampert* (2018), Art. 9 Rn. 14; *Weichert* (2020), Art. 9 Rn. 47.
391 *Schiff* (2018), Art. 9 Rn. 33.
392 *Weichert* (2020), Art. 9 Rn. 47.
393 *Bechmann,* Journal of Media Business Studies 2014, S. 21 (21 ff.); *Obar, Oeldorf-Hirsch,* Information, Communication & Society 2016, S. 1 (1 ff.); N*iedermann,* Allensbacher Archiv 2019, S. 1 (5).

liegt gerade mal bei 13 %, ganze 37 % gaben an, dass sie die Erklärungen überhaupt nicht lesen.[394] Die Gründe für das Nicht-Lesen sind vielfältig. Meist ist allerdings das Problem, dass die Erklärungen zu lang, zu kompliziert, zu unklar und damit für den durchschnittlichen Verbraucher kaum verständlich sind.[395] Eine Modellrechnung aus den USA hat bereits 2008 ergeben, dass knapp 30 Werktage (244 Std.) jährlich investiert werden müssten, um alle Datenschutzerklärungen/-bestimmungen zu lesen, denen man begegnet, wenn man ein Jahr im Internet surft.[396] Heute dürfte die notwendige Zeit noch um einiges höher liegen, bedenkt man, dass durch die DSGVO die Verbreitung und der Umfang von Datenschutzerklärungen gestiegen ist. Dies hat für betroffene Personen zur Folge, dass aufgrund von Unkenntnis in Praktiken eingewilligt wird, die diese sonst ablehnen würden. Eine Studie konnte eindrucksvoll belegen, dass die Teilnehmer fiktive AGBs und Datenschutzerklärungen überwiegend nicht lasen, diesen aber nichtsdestotrotz zustimmten, obwohl darinstand, dass die Daten mit der NSA ausgetauscht werden und das Erstgeborene als Bezahlung für die Nutzung des fiktiven Dienstes hergegeben werden muss.[397]

Neben der behindernden Länge und Komplexität kommt noch hinzu, dass viele Menschen das Gefühl haben, dass sie den Bestimmungen sowieso zustimmen müssen, wenn sie den Dienst nutzen wollen.[398] Ergänzend muss erwähnt werden, dass bspw. das Design von Einwilligungs-Tools auf Internetseiten einen wesentlichen, unterbewussten Einfluss auf die Erteilung von Einwilligungen hat.[399] Ebenso gibt es Hinweise, dass Datenschutzerklärungen häufig ungenau, unvollständig, widersprüchlich und unfair gegenüber der betroffenen Person sind.[400] Das hat zur Folge, dass einige Verantwortliche ggf. manipulativ die Freiwilligkeit untergraben und dass

394 *Europäische Kommission,* Special Eurobarometer 487a: The General Data Protection Regulation, 2019, S. 47 ff.

395 *Strahilevitz/Kugler*, Coase-Sandor Working Paper Series in Law and Economics 2016, S. 1 (2 ff.); N*iedermann,* Allensbacher Archiv 2019, S. 1 (7); *Europäische Kommission,* Special Eurobarometer 487a: The General Data Protection Regulation, 2019, S. 51; *Das et al.,* JMIR Mhealth Uhealth 2018, S. 1 (1 ff.).

396 *McDonald/Cranor,* A Journal of Law and Policy oft he Information Society 2008, S. 543 (563).

397 *Obar, Oeldorf-Hirsch,* Information, Communication & Society 2016, S. 1 (1 ff.).

398 N*iedermann,* Allensbacher Archiv 2019, S. 1 (7).

399 *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.).

400 *Benjumea et al.,* JMIR Mhealth Uhealth 2020, S. 1 (1 ff.); *Andow et al.,* Proceedings of the 28th USENIX Security Symposium 2019, S. 585 (585 ff.); *Rosenfeld et al.,* The

betroffene Personen Datenschutzerklärungen satt sind, da diese das Gefühl haben, dass ihnen keine Wahl gelassen wird.

Unter diesen Gesichtspunkten kann oftmals, besonders in Bezug auf die digitale Datenverarbeitung durch Apps, Internetseiten, Software etc., nicht von einer Einwilligung in freiwilliger und informierter Weise gesprochen werden.[401] Darum ist es notwendig, den Einwilligungsmechanismus als solchen neu zu definieren. Nur so kann die Einwilligung als Rechtsgrundlage auch zukünftig noch ernst zu nehmen sein und die Ziele der Freiwilligkeit und Informiertheit erfüllen. Zentral steht dabei die Forderung, dass betroffene Personen tatsächlich alle notwendigen Informationen in einer Art und Weise erhalten müssen, dass sie eine bewusste, aufgeklärte und freiwillige Entscheidung treffen können.

3. Die Einwilligung als Rechtsgrundlage für die Verarbeitung von Wesensdaten durch BCI

Grundsätzlich spricht nichts dagegen, dass die Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO als valide Rechtsgrundlage für die Verarbeitung von Wesensdaten durch BCI herangezogen wird. Solange die Vorgaben an die Freiwilligkeit, Transparenz, Zweckbindung und Form erfüllt sind, kann davon ausgegangen werden, dass die betroffene Person die mit der Verarbeitung von Wesensdaten einhergehenden Risiken ausreichend abschätzen und somit eine selbstbestimmte Entscheidung treffen kann, ob sie diese Risiken eingehen möchte.

Wie vorausgehend festgestellt wurde, werden die Vorgaben an eine rechtskräftige Einwilligung nur selten erfüllt. In Anbetracht der Verarbeitung von Wesensdaten durch BCI, könnte dies verheerende Auswirkungen für die betroffenen Personen und für die Gesellschaft haben. Stellt man sich bspw. vor, dass eine Person lediglich per Gedanke ein Online-Videospiel spielen möchte, dann allerdings unwissentlich einwilligt, dass ihre Wesensdaten auch dafür verwendet werden können, um diverse Auswertungen vorzunehmen (Verhalten, Meinung, psychische Belastbarkeit, Aufmerksamkeit etc.), wird ein enormes Potenzial für Missbrauch eröffnet.

American Journal of Geriatric Psychiatry 2017, S. 873 (873 ff.); *Huckvale/Torous/Larsen,* JAMA Network Open 2019, S. 1 (1 ff.).

401 In Bezug auf Consent-Banner auf Webseiten: *Loy/Baumgartner,* ZD 2021, S. 404 (408); *Voigt,* Die datenschutzrechtliche Einwilligung, 2020, S. 103 ff; *Martini et al.,* ZfDR 2021, S. 47 (55 f.); *Weinzierl,* NvWZ 2020, S. 1 (S. 8).

Dieses könnte ggf. darin bestehen, dass im Spiel platzierte visuelle Reize bei der betroffenen Person neurologische Reaktionen auslösen, die dann z.B. als Zustimmung oder Ablehnung ausgewertet werden können. Findet dies massenhaft statt, hätten bspw. Unternehmen die Möglichkeit, etliche Menschen zu kategorisieren und zu manipulieren. Um solche Potenziale erst gar nicht zu eröffnen, ist es notwendig, den Einwilligungsmechanismus entsprechend anzupassen. Nur dann könnte die Einwilligung als Rechtsgrundlage für die Verarbeitung von Wesensdaten einen ausreichenden Rahmen für eine informierte und selbstbestimmte Entscheidung der Betroffenen bieten.

4. Neurologisches Signal als datenschutzrechtliche Einwilligung

Neben der grundsätzlichen Anwendbarkeit von Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO stellt sich die Frage, ob Nutzer von BCI per neurologischem Signal eine rechtskräftige datenschutzrechtliche Einwilligung abgeben können.[402] Schließlich ist es denkbar, dass Nutzer, wenn sie bspw. per BCI durch das Internet surfen, auch per BCI in Datenverarbeitung einwilligen müssen. Um diese Frage zu beantworten, ist es notwendig, Art. 4 Nr. 11 DSGVO i.V.m. ErwG. 32 heranzuziehen. Art. 4 Nr. 11 DSGVO stellt die Anforderung, dass eine Einwilligung eine „unmissverständlich abgegebene Willensbekundung in Form einer […] eindeutigen bestätigenden Handlung" sein muss. Dies setzt ein explizites Tätigwerden der betroffenen Person voraus. ErwG. 32 konkretisiert diese Vorgabe und ergänzt, dass ein solches Tätigwerden z.B. vorliegt, wenn die betroffene Person aktiv ein Kästchen auf einer Internetseite auswählt oder bei Diensten der Informationsgesellschaft technische Einstellungen anpasst, während in Stillschweigen oder Untätigkeit keine eindeutig bestätigende Handlung zu sehen ist. Schlüssiges Verhalten ist somit nicht auszuschließen und kann als wirksame konkludente Einwilligung gezählt werden.[403]

Um diese Vorgaben auf neurologische Signale und deren Verarbeitung durch BCI anzuwenden, bedarf es einer genaueren Definition von einer „eindeutig bestätigenden Handlung". Relevant für die hier vorliegende Frage ist eingehend, was unter einer Handlung zu verstehen ist. Das Wort ‚Handlung' als solches ist eine Nominalisierung von ‚handeln'. Der Aus-

402 *Oettel*, PinG 2022, S. 136 (136 ff.).
403 *Klement* (2019), Art. 7 Rn. 35.

druck ‚handeln' hat seinen Ursprung in althochdeutschen ‚hantalōn', was so viel bedeutet wie „nach etwas greifen, in die Hand nehmen, bearbeiten".[404] Dieser wurde dann ins Mittelhochdeutsche zu ‚handeln' übertragen, was gemeinhin als „tätig sein, aktiv sein, vorgehen" definiert wird.[405] Gemäß der Wortherkunft beschreibt das Wort ‚Handlung' eine ausgeführte Tat.[406] Eine ausgeführte Tat wiederum manifestiert sich in einem Ergebnis. Eine Handlung ist demnach ein materialisiertes Tun. Diesem materialisierten Tun geht zwar ein Wille oder ein Gedanke bzw. ein neurologisches Signal voraus, allerdings führt nicht jedes neurologische Signal zu einer Handlung und ist somit auch nicht zwangsläufig mit dieser gleichzusetzen. Deutlich wird dies am psychologischen Phänomen des sog. Call of Void oder High place phenomenon. Dieses Phänomen beschreibt das weitverbreitete irrationale Bedürfnis einiger Menschen, springen zu wollen, wenn sie an einem Abgrund o.Ä. stehen.[407] Hier gibt es ein eindeutiges neurologisches Signal, was meist nicht in ein materialisiertes Tun übertragen wird. Neurologische Signale allein betrachtet sind somit nicht als Handlung zu definieren, da dazu das materialisierte Tun fehlt. In Kombination mit BCI hingegen ändert sich diese Tatsache. BCI ermöglichen Nutzern neue künstliche Formen von Outputs, die das natürliche komplexe Zusammenspiel zwischen Gehirn, Nervensystem und Muskeln umgehen,[408] somit nicht neurohormonell oder neuromuskulär sind und die herkömmlichen natürlichen Outputs entweder ersetzen, wiederherstellen, aufwerten, ergänzen oder verbessern können.[409] Dies bedeutet, dass zwischen dem Output von BCI aufgrund von neurologischen Signalen und dem gewöhnlichen neurohormonellen oder neuromuskulären Output defacto mindestens eine Ergebnisgleichheit besteht. Es macht somit keinen Unterschied, ob der Mauszeiger auf dem Bildschirm per Hand gesteuert und damit die Datenschutz-Einwilligungs-Checkbox angehakt wird oder per BCI und somit direkt per neurologischem Signal. Das zugrundeliegende neurologische Signal und das sich

404 Abrufbar unter: https://www.dwds.de/wb/handeln#1 (abgerufen 6.1.2025).
405 *Ebenda.*
406 Abrufbar unter: https://www.duden.de/rechtschreibung/Handlung (abgerufen 5.1.2025).
407 *Teismann et al.,* BMC Psychiatry 2020, S. 1 (1 ff.).
408 *Bae k et al.,* Computational Intelligence and Neuroscience 2019, S. 1 (1 f.); *Wolpaw/Winter Wolpaw,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 3 (6 ff.); *Mugdal et al.,* Interdisciplinary Neurosurgery 2020, S. 1 (2).
409 *Wolpaw/Winter Wolpaw,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 3 (3 f.).

manifestierende Ergebnis sind bei beiden Vorgehensweisen identisch. Lediglich die konkrete Umsetzung ist graduell unterschiedlich. Allerdings liegt kein kategorischer Unterschied vor, da in diesem konkreten Beispiel die Hand, als auch das BCI, im Grunde genommen lediglich Werkzeuge sind, um das neurologische Signal in das gewünschte manifestierte Ergebnis zu übertragen. BCI können neurologische Signale demnach ebenso in ein materialisiertes Tun übertragen, womit eine Handlung gemäß Art. 4 Nr. 11 DSGVO vorliegt.

Diese Handlung muss allerdings auch noch bestätigend sein. Bestätigend ist eine Handlung immer dann, wenn damit etwas aktiv als richtig oder zutreffend erklärt wird.[410] Wie aus ErwG. 32 hervorgeht, liegt eine bestätigende Handlung bspw. vor, wenn die betroffene Person aktiv ein Kästchen auf einer Internetseite auswählt oder bei Diensten der Informationsgesellschaft technische Einstellungen anpasst. Für eine rechtskräftige datenschutzrechtliche Einwilligung per BCI besteht demnach keine besondere Hürde. Wie bereits vorausgehend ausgeführt, besteht mindestens eine Ergebnisgleichheit zwischen einer Einwilligung per BCI und einer Einwilligung auf klassischem Wege. Wenn also eine gewöhnliche Einwilligung als bestätigend eingestuft wird, muss das Gleiche auch für eine Einwilligung per neurologischem Signal gelten. Solange mithilfe der Handlung etwas als zutreffend erklärt wird, ist diese Voraussetzung erfüllt.

Doch damit eine bestätigende Handlung als datenschutzrechtliche Einwilligung zählen kann, muss diese auch noch eindeutig sein. Eindeutig ist eine Handlung dann, wenn diese unmissverständlich keine andere Deutung der Intention zulässt als die beabsichtigte.[411] Wie bereits in Kapitel B.II. beschrieben, folgen BCI vier immer gleichbleibenden Schritten: 1. Signalaufzeichnung, 2. Extraktion von relevanten Signalen, 3. Übersetzung der relevanten Signale und 4. Output-Generierung.[412] In diesem Fall ist vor allem Schritt 3 relevant. In Schritt 3 findet mithilfe eines Übersetzungsalgorithmus eine Konvertierung der relevanten Signale zu entsprechenden Befehlen statt.[413] Beim Beispiel der Datenschutz-Einwilligung-Checkbox

410 Abrufbar unter: https://www.duden.de/rechtschreibung/bestaetigen (abgerufen 12.1.2022).

411 Abrufbar unter: https://www.duden.de/rechtschreibung/eindeutig (abgerufen 12.1.2022).

412 *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (270).

413 *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (272); detaillierter: *McFarland/Krusienski,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 147 (147 ff.).

auf einer Internetseite, müsste das BCI die vom Nutzer gewünschten Bewegungen des Mauszeigers und das ggf. gewünschte Anklicken der Checkbox korrekt aus den neurologischen Signalen herauslesen. Diese identifizierten Befehle werden abschließend an das externe Gerät weitergeleitet, welches dann den gewünschten Output erzeugt.[414] Da dieser Schritt auf technische Auswertungen und Umsetzungen angewiesen ist, besteht ein gewisses Fehlerpotential. So könnte es sein, dass bei der Übersetzung der neurologischen Signale Fehler passieren. Es könnte bspw. der Befehl zum Klicken fälschlicherweise als ‚nicht klicken' identifiziert werden o.Ä. Wie akkurat die Übersetzung ist, hängt häufig davon ab, welche Methode gewählt wird.[415] Die genausten Übersetzungen liefern Neurale Netze und Deep-Learning Algorithmen.[416] Mit diesen Methoden können Genauigkeiten bis zu 92[417]-97 %[418] erreicht werden. Allerdings sind diese Aussagen nur bedingt belastbar. Entweder ist die Teilnehmerzahl bei entsprechenden Studien sehr niedrig oder die Neuronalen Netze und Deep Learning Algorithmen werden mit einem limitierten Datensatz trainiert.[419] Hinzu kommt, dass auch die Erfahrung der Nutzer im Umgang mit BCI eine Rolle bei der Genauigkeit der Signalübersetzung spielen könnte. Nutzer mit wenig Erfahrung sind im Schnitt ungenauer in der Handhabung von BCI als erfahrene Nutzer.[420] In Anbetracht dieser Störvariablen ist es fraglich, ob Einwilligungen per BCI konsistent die notwendige Eindeutigkeit zugesprochen werden kann.

Grundsätzlich ist es möglich, per BCI eine rechtskräftige datenschutzrechtliche Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO abzugeben. Neurologische Signale und deren durch BCI erzeugten Outputs können als Handlung definiert werden und diese Handlungen können bestäti-

414 *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (272).

415 *Aggrawal/Chugh,* Array 2019, S. 1 (7).

416 *Schwemmer et al.,* nature medicine 2018, S. 1669 (1669 ff.); *Korovesis et al.,* Electronics 2019, S. 1 (10 ff.); *Shan/Liu/Stefanov,* Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence 2018, S. 1604 (1608 f.); *Aggrawal/Chugh,* Array 2019, S. 1 (7); *Jana/Swetapadma/Pattnaik,* Ain Shams Engineering Journal 2018, S. 2871 (2875 ff.).

417 *Korovesis et al.,* Electronics 2019, S. 1 (10 ff.).

418 *Jana/Swetapadma/Pattnaik,* Ain Shams Engineering Journal 2018, S. 2871 (2875 ff.).

419 Bzgl. Problem könnte Augmented Data in Zukunft zu besseren Datensätzen führen: *Zhang/Liu*, Improving brain computer interface performance by data augmentation with conditional Deep Convolutional Generative Adversial Networks, v. 19.6.2018, *https://arxiv.org/abs/1806.07108* (abgerufen 12.1.2022).

420 *Rasmussen/Acharya/Thakor,* Proceedings of the IEEE 32nd Annual Northeast Bioengineering Conference 2006, S. 167 (167 f.).

gend sein. Allerdings mangelt es derzeit an der allgemeinen vorhandenen Eindeutigkeit. Damit ein neurologisches Signal, welches mithilfe eines BCI in ein materialisiertes Tun übertragen wird, allgemein eindeutig ist, bedarf es normierter, robuster und zuverlässiger Systeme und einen gewissen Grad an Erfahrung auf Seiten der Nutzer. Beides kann derzeit noch nicht flächendeckend vorausgesetzt werden. Damit können Einwilligungen per BCI nur einzeln betrachtet als DSGVO-konform eingestuft werden, was in Zukunft unpraktikabel ist. Demnach bedarf er regulatorischer Maßnahmen, um einen Rahmen zu schaffen, der besagt, ab wann Einwilligungen mithilfe von BCI als eindeutig definiert werden können.

5. Neurologisches Signal als datenschutzrechtliche Einwilligung bei besonderen Kategorien von personenbezogenen Daten

In Bezug auf besondere Kategorien von personenbezogenen Daten, werden die Wirksamkeitsvoraussetzungen durch Art. 9 Abs. 2 lit. a DSGVO um das Merkmal der Ausdrücklichkeit ergänzt. Die Einwilligung muss sich demnach ausdrücklich auf die Verarbeitung von besonderen Kategorien von personenbezogenen Daten beziehen und die konkludente Einwilligung wird für alle Daten, die unter Art. 9 Abs. 1 DSGVO fallen, ausgeschlossen.[421] Im Grunde verschärft der Gesetzgeber damit die Anforderung an die Eindeutigkeit einer datenschutzrechtlichen Einwilligung in Bezug auf besondere Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO. Sobald diese auf Grundlage einer Einwilligung verarbeitet werden sollen, muss die betroffene Person demnach noch unmissverständlicher und pointierter einwilligen als bei anderen Daten. Dementsprechend wird, aufgrund der bereits genannten Probleme mit Bezug auf die Eindeutigkeit, eine rechtskräftige Einwilligung mithilfe eines BCI noch mehr ausgeschlossen. Auch hier bedarf es weitere technologische und gesellschaftliche Entwicklungen sowie eine rechtliche Regulation, damit in Zukunft per neurologischem Signal ausdrücklich in die Verarbeitung von besonderen Kategorien von personenbezogenen Daten eingewilligt werden kann.

421 *Kampert* (2018), Art. 9 Rn. 14; *Weichert* (2020), Art. 9 Rn. 47.

6. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO: Berechtigtes Interesse

Neben der datenschutzrechtlichen Einwilligung ist es in Zukunft ebenso denkbar, dass das berechtigte Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO als Rechtsgrundlage für die Verarbeitung von Wesensdaten herangezogen wird. Denn wie in Kapitel H.I.3 dargelegt wurde, ist es denkbar, dass Wesensdaten nicht kategorisch unter Art. 9 Abs. 1 DSGVO gezählt werden könnten, womit das berechtigte Interesse als legitime Rechtsgrundlage nicht ausgeschlossen wird. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO besagt, dass eine Verarbeitung von personenbezogenen Daten auch dann rechtmäßig sein kann, wenn diese für die Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Allerdings ist eine solche Rechtfertigung einer Datenverarbeitung nur möglich, wenn damit keine Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Diesem Umstand ist insbesondere dann Rechnung zu tragen, wenn es sich bei der betroffenen Person um ein Kind handelt. Damit hat der Gesetzgeber eine Interessenabwägung als Auffangklausel in die abschließende Aufzählung der Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten eingebaut.[422] Allerdings kann diese Rechtsgrundlage nicht von Behörden genutzt werden, wie Art. 6 Abs. 1 UAbs. 2 DSGVO konkretisiert. Ebenso ist das berechtigte Interesse bei der Verarbeitung von besonderen Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 2 DSGVO als valide Rechtsgrundlage ausgeschlossen.

Gemäß der Formulierung von Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO muss das Interesse drei Anforderungen erfüllen: 1. Es muss berechtigt sein, 2. Es muss erforderlich sein und 3. Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen dürfen nicht überwiegen. Um diese Rechtsgrundlage auf die Verarbeitung von Wesensdaten anzuwenden, bedarf es einer eingehenden Analyse dieser drei Anforderungen.

a. Berechtigt

Wann genau ein berechtigtes Interesse vorliegt, wird nicht weitergehend von der DSGVO konkretisiert. Die im Normtext verwendete Formulierung

422 *Buchner/Petri* (2020), Art. 6 Rn. 141; *Schantz* (2019), Art. 6 Rn. 86; Anderer Meinung: *Frenzel* (2021), Art. 6 Rn. 26; *Taeger* (2019), 4. Aufl. Art. 5 Rn. 26.

lässt aber logischerweise darauf schließen, dass das verfolgte Interesse des Verantwortlichen oder eines Dritten zumindest rechtmäßig sein muss.[423] ErwG. 47 ff. nennen zwar mögliche Beispiele von berechtigten Interessen,[424] allerdings grenzen diese den Anwendungsbereich kaum sinnvoll ein. Demzufolge besteht erstmal ein weites Verständnis bei der Bewertung von berechtigten Interessen.[425] Somit kann theoretisch jedes rechtliche, wirtschaftliche oder auch ideelle Interesse als berechtigt eingestuft werden.[426] Das Bundesverwaltungsgericht stellte 2019 allerdings fest, dass Interessen nur dann berechtigt sind, wenn diese „schutzwürdig und objektiv begründbar" sind.[427] Objektiv begründbar könnte ein Interesse regelmäßig dann sein, wenn es sinnvollerweise zweckmäßig ist,[428] keine alternative Rechtsgrundlage vorliegt und keine andere Möglichkeit der Erreichung der Interessen besteht, die ohne Verarbeitung von personenbezogenen Daten auskommt (bspw. Verarbeitung von anonymisierten Daten).[429] Schutzwürdig könnten wiederum Grundrechte wie z.B. Meinungs- und Pressefreiheit sein, aber auch Forschungstätigkeiten, die Ausübung sowie Verteidigung von Rechtsansprüchen, der Schutz vor böswilligen Dritten oder die Gewinnsteigerung/-stabilisierung, Effizienzsteigerung, Kostensenkung und Optimierung von Prozessen.[430]

b. Erforderlich

Das Interesse muss aber nicht nur berechtigt, sondern die dafür notwendige Datenverarbeitung auch noch erforderlich sein. Diese Anforderung ist nur dann erfüllt, wenn es keine andere gleichwertige Möglichkeit der Interessenserreichung gibt, die milder und weniger invasiv für die betrof-

423 *Spindler/Dalby* (2019), Art. 6 DSGVO Rn. 14; *Schulz* (2018), Art. 6 Rn. 57; *Heberlein* (2018), Art. 6 Rn. 25.

424 Wenn bereits eine Beziehung zwischen Verantwortlichem und Betroffenen besteht, Betrugsverhinderung, Direktwerbung, IT-Sicherheit, Datenaustausch in einer Unternehmensgruppe.

425 *Frenzel* (2021), Art. 6 Rn. 28; *Schantz* (2019), Art. 6 Rn. 98.

426 *Schulz* (2018), Art. 6 Rn. 57; *Buchner/Petri* (2020), Art. 6 Rn. 146a; *Schantz* (2019), Art. 6 Rn. 98.

427 BVerwG Urt. v. 27.3.2019 – 6 C 2/18, DuD 2019, 518 (522).

428 *Spindler/Dalby* (2019), Art. 6 DSGVO Rn. 14.

429 *Schulz* (2018), Art. 6 Rn. 57.

430 *Buchner/Petri* (2020), Art. 6 Rn. 147; *Reimer* (2018), Art. 6 Rn. 55; *Datenschutzkonferenz,* Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 12.

fenen Personen ist.[431] So könnte bspw. eine Verarbeitung anonymer oder anonymisierter Daten oftmals eine gleichwertige Alternative zur geplanten Verarbeitung darstellen, womit die Erforderlichkeit nicht mehr gegeben wäre.[432] Analog kann hierbei die enge Auslegung des Begriffs aus der Rechtsprechung zu Art. 7, 8 GRCh angewandt werden, aus der hervorgeht, dass eine Erforderlichkeit nur dann vorliegt, wenn „die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige" beschränkt werden.[433] Demnach kann sich die Erforderlichkeit des Interesses nicht grundsätzlich aus wirtschaftlichen Aspekten (kostengünstiger, effizienter etc.) ergeben.[434] Notwendig ist allerdings, dass bei der Beurteilung der gleichwertigen Möglichkeiten der Interessenserreichung auch die realistische Zumutbarkeit für den Verantwortlichen Berücksichtigung findet.[435] Somit könnten bei Verantwortlichen, die über ausreichend finanzielle Mittel verfügen, geplante Verarbeitungen, welche zwar preiswerter, aber nicht milder sind als mögliche Alternativen, als nicht erforderlich für die Interessenserreichung eingestuft werden, während für weniger liquide Verantwortliche das Gegenteil gilt.

c. Interessenabwägung

Wenn ein berechtigtes Interesse auf Seiten des Verantwortlichen vorliegt und die Datenverarbeitung dafür erforderlich ist, muss abschließend noch eine Abwägung mit den Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen stattfinden. Einschlägige Rechte könnten bspw. die informationelle Selbstbestimmung, unternehmerische Freiheit, Berufsfreiheit, das Teilhaberecht und die Würde des Menschen sein.[436] Relevante Interessen von betroffenen Personen könnten wiederum sein, keine wirtschaftlichen Nachteile zu erleiden oder nicht das Ansehen in der Öffentlichkeit zu verlieren.[437] Damit der Verantwortliche eine Interes-

431 *Schantz* (2019), Art. 6 Rn. 100; *Datenschutzkonferenz,* Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 13.
432 *Schulz* (2018), Art. 6 Rn. 57.
433 EuGH, Urt. v. 4.5.2017- C-13/16 (Rīgas satiksme), BeckRS 2017, Rn. 30; *Schantz* (2019), Art. 6 Rn. 100; *Buchner/Petri* (2020), Art. 6 Rn. 147a.
434 *Schantz* (2019), Art. 6 Rn. 100; *Buchner/Petri* (2020), Art. 6 Rn. 147a.
435 *Taeger* (2019), 4. Aufl. Art. 5 Rn. 36.
436 *Reimer* (2018), Art. 6 Rn. 60; *Buchner/Petri* (2020), Art. 6 Rn. 148; *Schantz* (2019), Art. 6 Rn. 101.
437 *Buchner/Petri* (2020), Art. 6 Rn. 148a; *Schantz* (2019), Art. 6 Rn. 101.

senabwägung durchführen kann, ist es somit wichtig, dass die vorliegenden Interessen und tangierten Rechte des Verantwortlichen und der Betroffenen klar definiert sind. Sobald dies geschehen ist, müssen die jeweiligen Interessen und Rechte gewichtet werden.[438] Für eine solche Gewichtung sind vor allem die Invasivität der Verarbeitung, die möglichen Auswirkungen der Verarbeitung, die Kategorien der betroffenen Daten, die Kategorien und der Umfang der betroffenen Personen, die Beziehung zwischen Verantwortlichem und Betroffenen, der Zweck der Verarbeitung und vorhandene technische und organisatorische Maßnahmen, um das Risiko für die betroffenen Personen zu minimieren, maßgeblich.[439] ErwG. 47 S. 3 f. ergänzt diese Kriterien und stellt fest, dass der Verantwortliche bei einer solchen Interessenabwägung ebenso die vernünftigen Erwartungen der Betroffenen berücksichtigen muss. Sobald betroffene Personen aufgrund der Umstände und der Situation nicht vernünftigerweise mit einer weiteren Verarbeitung ihrer Daten rechnen müssen, könnte laut ErwG. 47 S. 4 oftmals davon ausgegangen werden, dass das Interesse der Betroffenen überwiegt.

Ziel der Abwägung ist es, mögliche unverhältnismäßige Folgen für betroffene Personen zu identifizieren. Nur wenn diese vorliegen, überwiegen die Interessen der Betroffenen, womit die Verarbeitung im Zweifel nicht direkt als unrechtmäßig zu bewerten ist.[440] Fälle, in denen die Interessen der betroffenen Personen oftmals überwiegen könnten, sind bspw. die Erstellung von Persönlichkeitsprofilen und die umfangreiche Verarbeitung von Bewegungs- und Nutzungsdaten.[441] Ebenso überwiegen die Interessen der Betroffenen meistens dann, wenn es sich bei den Betroffenen um Kinder handelt.

7. Das berechtigte Interesse als Rechtsgrundlage für die Verarbeitung von Wesensdaten durch BCI

Wie bereits in Kapitel H.I.2 festgestellt wurde, können Wesensdaten nicht pauschal als besondere Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO definiert werden. Damit fallen Wesensdaten auch

438 *Schulz* (2018), Art. 6 Rn. 59.
439 *Spindler/Dalby* (2019), Art. 6 DSGVO Rn. 19; *Buchner/Petri* (2020), Art. 6 Rn. 150 ff.; *Schulz* (2018), Art. 6 Rn. 59; *Reimer* (2018), Art. 6 Rn. 60 ff; *Heberlein* (2018), Art. 6 Rn. 28.
440 *Reimer* (2018), Art. 6 Rn. 63.
441 *Buchner/Petri* (2020), Art. 6 Rn. 153.

nicht kategorisch unter den besonderen Schutz des Art. 9 DSGVO, womit das berechtigte Interesse als Rechtsgrundlage nicht prinzipiell ausgeschlossen ist. Inwiefern dies für die Praxis und für betroffene Personen relevant sein könnte, soll hier anhand eines realistischen Beispiels diskutiert werden. Dafür muss erst analysiert werden, wie das berechtigte Interesse momentan häufig als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten verwendet wird.

a. Das berechtigte Interesse in der derzeitigen Praxis

In der derzeitigen Praxis wird das berechtigte Interesse häufig genutzt, wenn es darum geht, Online-Dienste zu optimieren. So stützt sich Amazon bspw. auf das berechtigte Interesse, um die Amazon-Dienste zu verbessern und um interessensbasierte Produktvorschläge zu schalten.[442] Facebook beruft sich wiederum auf das berechtigte Interesse, um Messungen und Analysen für Werbekunden durchzuführen.[443] Auch der Cloud-Storage-Anbieter Dropbox beruft sich auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO, um zu erfahren, wie Nutzer mit den Diensten interagieren und um diese zu verbessern.[444] Was genau unter „verbessern" und „personalisieren" zu verstehen ist, wird dabei allgemein nicht spezifiziert. Somit ist davon auszugehen, dass Unternehmen das berechtigte Interesse momentan häufig als Auffangklausel nutzen, um Datenverarbeitungen, wie bspw. die umfangreiche Erstellung und Auswertung von Nutzer- und Werbeprofilen, die nicht mit einer Einwilligung oder mithilfe eines zugrundeliegenden Vertrags gerechtfertigt werden können, zu legitimieren.

Am Beispiel Facebook wird deutlich, welche Folgen solche Auswertungen, die sich großteils auf das berechtigte Interesse, den Dienst zu „verbessern" oder zu „personalisieren", stützen, haben können. 2018 wurde der Algorithmus der Social-Media Seite angepasst, um die Nutzer-Interaktion mit dem Dienst zu erhöhen. Das Ziel wurde erreicht. Allerdings führte die Anpassung scheinbar auch dazu, dass negative Postings und wütende Reaktionen mit Reichweite und Aufmerksamkeit belohnt wurden, womit

442 Abrufbar unter https://www.amazon.de/gp/help/customer/display.html?nodeId=TcxwSYJNmpQYGgNWkX (abgerufen 4.1.2025).

443 Abgerufen unter https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 (abgerufen 4.1.2025).

444 Abgerufen unter https://help.dropbox.com/de-de/accounts-billing/security/privacy-policy-faq (abgerufen 12.3.2022).

die Plattform insg. toxischer wurde.[445] So stellten Nutzer in Indien bspw. fest, dass ihnen immer mehr Inhalte angezeigt wurden, die zu Konflikten, Hass und Gewalt aufforderten. Es ist davon auszugehen, dass dies eine wesentliche Rolle bei den gewaltsamen Protesten im Februar 2020 in Indien gespielt hat.[446] Erschwerend kommt hinzu, dass die Auswertung der Nutzer und die entsprechenden Anpassungen der Dienste dazu geführt haben könnten, dass einer von acht Nutzern der Plattform ein zwanghaftes Nutzungsverhalten aufweist, welches sich negativ auf den Schlaf, die Arbeit und die Familie/Beziehung auswirken könnte.[447] Aus Facebooks Perspektive ist der Dienst besser und personalisierter geworden, wenn viele Menschen die Plattform häufig und intensiv nutzen. Für die Nutzer kann dieses berechtigte Interesse des Unternehmens allerdings ernstzunehmende Folgen haben. Ob der Verarbeitung auf Grund des berechtigten Interesses eine ordnungsgemäße und notwendige Interessenabwägung vorangegangen ist, ist zweifelhaft. Allerdings zeigt dieses Beispiel sehr gut, wie die Rechtsgrundlage aus Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO derzeit Anwendung findet.

b. Beispielhafte Interessenabwägung bei der Verarbeitung von Wesensdaten

Wie bereits dargestellt, findet das berechtigte Interesse in der derzeitigen Praxis häufig Anwendung, wenn Dienste verbessert oder personalisiert werden sollen. Um der gängigen Praxis zu entsprechen, soll an dieser Stelle eben jenes Interesse eines Verantwortlichen bei der Verarbeitung von Wesensdaten Grundlage für eine beispielhafte Interessenabwägung sein.

Um diesen beispielhaften Fall aussagekräftiger zu gestalten, soll der Verantwortliche und dessen Interesse spezifiziert werden. Der exemplarische Verantwortliche ist Anbieter einer Social-Media Anwendung und das zugrundeliegende berechtigte Interesse ist, die Anwendung zu verbessern und zu personalisieren. Explizit sind darunter folgende Inhalte zu subsumieren:

---

445 *Hagey/Horwitz,* Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead., v. 15.9.2021, https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215#refreshed?mod=article_inline (abgerufen 12.3.2022).

446 *Purnell/Horwitz,* Facebook Services Are Used to Spread Religios Hatred in India, Internal Documents Show, v. 23.10.2021, https://www.wsj.com/articles/facebook-services-are-used-to-spread-religious-hatred-in-india-internal-documents-show-11635016354?mod=article_inline (abgerufen 12.3.2022).

447 *Wells/Seetharaman/Horwitz,* Is Facebook Bad for You? It Is for About 350 Million Users, Company Survery Suggest, v. 5.11.2021, https://www.wsj.com/articles/facebook-bad-for-you-360-million-users-say-yes-company-documents-facebook-files-11636124681#refreshed?mod=article_inline (abgerufen 12.3.2022).

- Personalisierter Feed: Anzeigen von Inhalten, die den Nutzer tatsächlich interessieren
- Interaktion steigern: Anzeigen von Inhalten, mit denen der Nutzer eher interagiert
- Vorbeugung von nachteilhaften Nutzungsmustern: Anzeigen von sorgfältig aufeinander abgestimmten Inhalten, die den Nutzer eher davon abhalten, zwanghafte Nutzungsmuster zu entwickeln und vielmehr eine langfristige und konsistente Nutzung der Anwendung bewirken sollen
- Steigerung der Sicherheit der Anwendung: Bessere Identifikation von schädlichen und rechtswidrigen Inhalten

Das verfolgte Interesse ist nicht rechtswidrig. Ebenso ist es objektiv begründbar, da die Verarbeitung von Wesensdaten sinnvollerweise für die Zweckerfüllung notwendig ist und es keine vergleichbare Datenquelle mit einer solchen Qualität gibt. Ebenso ist das Interesse schutzwürdig, da vor allem eine Gewinnsteigerung/-stabilisierung, Effizienzsteigerung und Optimierung von Prozessen des Verantwortlichen erreicht werden würden. Ein derartiges Interesse einer Social Media-Anwendung ist demnach als legitimes berechtigtes Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zu definieren.

Allerdings muss das Interesse auch erforderlich sein. Um die Erforderlichkeit des Interesses zu diskutieren, bedarf es einer inhaltlichen Konkretisierung der geplanten Datenverarbeitung. Um das berechtigte Interesse zu erreichen, sollen Wesensdaten von Nutzern verarbeitet werden, die den Dienst mittels eines BCI nutzen. Dabei sollen aggregierte und individuelle neurologische Reaktionen auf Inhalte erhoben und verarbeitet werden. Individuelle neurologische Reaktionen sind bspw. das Interesse oder die Ablehnung gegenüber Inhalten und die Wahrnehmung von Likes, Shares und Kommentaren. Dabei werden nur so viele neurologische Reaktionen verarbeitet, wie notwendig, um statistisch belastbare Aussagen treffen zu können. Somit werden nicht alle Reaktionen auf alle angeschauten Inhalte erhoben und verarbeitet, sondern eine möglichst begrenzte Menge. Diese Wesensdaten werden dann genutzt, um einen vollkommen individuellen, auf den Nutzer abgestimmten Feed zu erstellen. Dieser besteht dann aus Inhalten, die den Nutzer interessieren, begeistern, zur Interaktion motivieren, von schädlichen Nutzungsmustern abhalten und diesen langfristig und konsistent an die Anwendung binden. Die erhobenen individuellen neurologischen Reaktionen werden jeweils nach einem Monat vollständig gelöscht. Die erstellten Auswertungen werden nach drei Monaten gelöscht, um einen Abgleich mit älteren Auswertungen zu ermöglichen und die

Weiterentwicklung des Feeds zu gewährleisten. Aggregierte anonyme neurologische Reaktionen werden ergänzend genutzt, um allgemein auszuwerten, welche Inhalte bspw. eher auf Ablehnung stoßen bzw. eher toxisches Verhalten erzeugen. Diese Informationen werden dann verwendet, um die angezeigten Inhalte sorgfältig aufeinander abzustimmen, damit Nutzer keine schädlichen Nutzungsmuster entwickeln. Ebenso werden die Daten genutzt, um schädliche und rechtswidrige Inhalte besser zu erkennen und zu beseitigen. Die aggregierten Daten werden in anonymisierter Form unbegrenzt gespeichert.

Um die genannten Interessen zu erreichen, kann argumentiert werden, dass es dafür keine gleichwertige und dem Verantwortlichen zumutbare alternative Möglichkeit gibt, welche milder und weniger invasiv für die betroffene Person ist. Die Verarbeitung von Wesensdaten bietet in diesem Fall eine Genauigkeit, die mit keiner anderen möglichen Datenart erreicht werden kann. Würde man alternativ auf Likes, Kommentare und Shares ausweichen, um verlässlich Interesse und Ablehnung der Nutzer zu identifizieren sowie die bessere Erkennung von schädlichen und rechtswidrigen Inhalten zu erreichen, würde man nicht ansatzweise gleichwertige Ergebnisse erhalten. Likes, Kommentare und Shares bilden nicht zwangsläufig Interesse oder Ablehnung ab und verzerren so das Ergebnis. Hinzu kommt, dass eine Vorbeugung von nachteilhaften Nutzungsmustern aus gleichen Gründen ohne Wesensdaten deutlich schwieriger wird. Ebenso ist anzumerken, dass die verarbeiteten Wesensdaten, wenn möglich anonymisiert werden. Bei den Wesensdaten, die für den individuellen Feed notwendig sind und somit nicht anonymisiert werden können, wird die Verarbeitung und die Speicherung auf das absolut Notwendige beschränkt. Auch ergibt sich die Erforderlichkeit nicht ausschließlich aus wirtschaftlichen, sondern auch aus gemeinwohldienlichen (Erkennung von schädlichen und rechtswidrigen Inhalten) und nutzerbegünstigenden (Verhinderung von nachteilhaften Nutzungsmustern) Aspekten. Demzufolge kann festgestellt werden, dass das berechtigte Interesse des Verantwortlichen auch als erforderlich angesehen werden kann.

Wenn ein berechtigtes Interesse auf Seiten des Verantwortlichen vorliegt und die Datenverarbeitung dafür erforderlich ist, muss abschließend noch eine Abwägung mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen stattfinden. Dafür sollte einführend betrachtet werden, welche Daten und welche Personen genau betroffen sind, wie invasiv die Verarbeitung ist, welche möglichen Auswirkungen die Verarbeitung haben könnte, welche Beziehung zwischen Verantwortlichen und

Betroffenen besteht und inwiefern die Verarbeitung mit den vernünftigen Erwartungen der Betroffenen übereinstimmt.

Von der Verarbeitung sind Wesensdaten betroffen. Explizit geht es um vereinzelte neurologische Reaktionen auf Inhalte. Diese Daten werden nur von jenen Nutzern verarbeitet, die mithilfe eines BCI mit der Anwendung interagieren. Da die Anwendung prinzipiell nur von Erwachsenen genutzt werden darf, sind demnach keine Kinder von der Verarbeitung betroffen.

Grundsätzlich bringt diese Verarbeitung von Wesensdaten zwar eine vergleichsweise hohe Invasivität mit sich, allerdings werden die explizit erhobenen Wesensdaten nicht dazu genutzt, um gezielt sensitive Informationen der Nutzer zu erhalten, sondern, um Interesse und Ablehnung zu identifizieren. Dass eine umfangreiche Identifizierung von Interesse und Ablehnung vor allem bei Social Media-Anwendungen möglich ist, ist bekannt[448] und auch gängige Praxis.[449] In Verbindung mit Wesensdaten werden die Aussagen dieser Praxis lediglich genauer, womit aber keine kategorisch neue Form von Datenverarbeitung vorliegt. Zwar sind Wesensdaten betroffen, aber da die Verarbeitung auf das notwendige Maß beschränkt ist, kann festgestellt werden, dass eine vergleichbare Invasivität der Verarbeitung zur bereits gängigen Praxis besteht. Demnach liegt hier kein Hindernis für die geplante Verarbeitung vor.

Ergänzend sind auch mögliche Auswirkungen der Verarbeitung zu betrachten. Die grundsätzliche Auswirkung der Verarbeitung für die betroffene Person ist ein personalisierter Feed, gesteigerte Interaktion und Schutz vor nachteilhaften Nutzungsmustern. Wie in Kapitel D.I bereits dargelegt wurde, weisen Wesensdaten ein umfangreiches Informationsschöpfungspotential auf. Neurologische Signale lassen demnach eine Vielzahl von Rückschlüssen auf die betroffene Person zu. Auch Informationen zu Interesse und Ablehnung bzgl. Inhalten können bei Missbrauch bspw. Rückschlüsse zur politischen Meinung, Sexualität und weltanschaulichen Überzeugung zulassen. Allerdings tritt diese Auswirkung nur auf, wenn die Daten unerlaubterweise zweckentfremdet oder entwendet werden. Dies ist zwar ein bestehendes Risiko, aber nicht eine prinzipiell mögliche Auswirkung der gewöhnlichen zweckgerichteten Datenverarbeitung. Auch hier kann demnach festgestellt werden, dass die möglichen Auswirkungen für Betroffene

448 *Kosinski/Stillwell/Greapel,* PNAS 2013, S. 5802 (5803 f.); *Youyuo/Kosinski/Stillwell,* PNAS 2014, S. 1036 (1037 f.).

449 Abgerufen unter https://www.broadbandsearch.net/blog/what-facebook-knows-about-me#post-navigation-9 (abgerufen 27.3.2022).

überschaubar sind und kein Hindernisgrund für die Verarbeitung darstellen.

Nichtsdestotrotz ist weiterhin auch die Beziehung zwischen den Akteuren zu beachten. Da es sich um eine Social Media-Anwendung handelt, besteht kein Abhängigkeitsverhältnis zwischen Verantwortlichen und Betroffenen im klassischen Sinne. Betroffene nehmen ein Angebot wahr, welches vom Anbieter bereitgestellt wird. Den betroffenen Personen steht es jederzeit frei, den Dienst zu verlassen und ihr Konto zu löschen. Ebenso haben sie jederzeit die Möglichkeit, Gebrauch von ihren Betroffenenrechten zu machen. Auch die Beziehung zwischen Verantwortlichen und Betroffenen ist damit kein Ausschlussgrund für das berechtigte Interesse.

Bzgl. der Sicherheit der Verarbeitung hat der Verantwortliche, wenn möglich, Anonymisierungen implementiert und die Verarbeitung der Wesensdaten auf das notwendigste Maß beschränkt. Für diesen beispielhaften Fall wird auch davon ausgegangen, dass der Verantwortliche weitere umfangreiche technische und organisatorische Maßnahmen ergriffen hat, um eine hohe Datensicherheit zu gewährleisten.

Zu guter Letzt ist noch auf die vernünftige Erwartung der Betroffenen abzustellen. Es ist hinreichend bekannt, dass bei der Nutzung einer Social Media-Anwendung umfangreiche personenbezogene Daten verarbeitet werden, meist um den Dienst zu personalisieren und zu verbessern.[450] Die betroffene Person kann somit vernünftigerweise erwarten, dass dies auch für alternative Plattformen gilt.

Abschließend und zentral für die eigentliche Interessenabwägung ist die Betrachtung der vorhandenen Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen. Bei der Nutzung einer Social Media-Anwendung kann grundsätzlich behauptet werden, dass Nutzer interessiert daran sind, verlässlich für sie relevante Informationen zu erhalten. Ebenso besteht das Interesse, keine nachteilhaften Nutzungsmuster zu entwickeln, und dass nicht unnötig viele personenbezogene Daten verarbeitet werden. Alle vorliegenden Interessen lassen sich theoretisch mit den Interessen und dem Vorgehen des Verantwortlichen vereinbaren. Relevanter sind jedoch die betroffenen Grundrechte und Grundfreiheiten. Zwei wesentliche Grundrechte der betroffenen Personen sind von der Verarbeitung betroffen, welche sich nachteil- sowie vorteilhaft auswirken. Nachteilhaft für die betroffene Person ist, dass durch die Datenverarbeitung ihr Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh tangiert wird. Vorteilhaft

450 Abgerufen unter https://www.broadbandsearch.net/blog/what-facebook-knows-about-me#post-navigation-9 (abgerufen 27.3.2022).

ist wiederum, dass mit der Verhinderung von nachteilhaften Nutzungsmustern die körperliche und geistige Unversehrtheit i.S.v. Art. 3 Abs. 1 GRCh geschützt wird. Grundsätzlich ist dabei die körperliche und geistige Unversehrtheit als wichtiger einzustufen als der Schutz der personenbezogenen Daten, womit in der Bilanz ein vorteilhaftes Ergebnis für die betroffene Person vorliegt.

Zusammenfassend kann demnach festgestellt werden, dass bei diesem praxisnahen Beispiel einer möglichen Anwendung des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in Bezug auf Wesensdaten durchaus zu dem Schluss gekommen werden kann, dass die Verarbeitung keine unverhältnismäßigen Folgen für betroffene Personen mit sich bringt und somit als rechtmäßig einzustufen ist.

c. Abschließende Einschätzung zum berechtigten Interesse als Rechtsgrundlage für die Verarbeitung von Wesensdaten

Wie mit diesem vereinfachten Beispiel gezeigt werden konnte, gibt es Möglichkeiten, die Verarbeitung von Wesensdaten über das berechtigte Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zu rechtfertigen. Dies stellt so lange kein Problem dar, wie Verantwortliche gewissenhaft die notwendigen Interessenabwägungen durchführen und sich an die festgelegten Zwecke der Datenverarbeitung halten. Wie aus der vorherigen kurzen Darstellung der derzeit gängigen Praxis am Beispiel von Facebook hervorgegangen ist, kann diese Gewissenhaftigkeit von Verantwortlichen allerdings nicht allgemein vorausgesetzt werden. Vielmehr ist davon auszugehen, dass das berechtigte Interesse auch in Bezug auf Wesensdaten als Auffangklausel ausgenutzt werden könnte, um umfangreichere und sensitivere Auswertungen von Wesensdaten, die nicht mit einer Einwilligung oder mithilfe eines zugrundeliegenden Vertrags gerechtfertigt werden können, scheinbar zu legitimieren. Erschwerend kommt hinzu, dass mit der alleinigen Möglichkeit von Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO als valide Rechtsgrundlage für die Verarbeitung von Wesensdaten, das Risiko von missbräuchlicher Verarbeitung der betroffenen Daten steigt. Welche Sprengkraft eine missbräuchliche Verarbeitung von Wesensdaten haben könnte, sollte mittlerweile deutlich geworden sein.

Gemäß dieser Erkenntnis zeigt sich erneut, dass Wesensdaten prinzipiell vom besonderen Schutz des Art. 9 DSGVO erfasst werden sollten. Damit würde das berechtigte Interesse als valide Rechtsgrundlage ausgeschlossen

werden, womit eine unnötig umfangreiche Verarbeitung von Wesensdaten vermieden wird.

H. Betroffenenrechte: Das Auskunftsrecht

I. Allgemeines

Sobald eine Datenverarbeitung gerechtfertigt ist, muss es der betroffenen Person ermöglicht werden, die Verarbeitung zu überprüfen bzw. anzupassen. Die DSGVO sieht darum umfangreiche Rechte für Betroffene vor. In Bezug auf BCI und die zukünftige Verarbeitung von Wesensdaten ist besonders das Auskunftsrecht nach Art. 15 DSGVO relevant. Darum soll an dieser Stelle der Fokus auf eben jenem Recht liegen.

Das Auskunftsrecht nach Art. 15 DSGVO ist eine explizite Vertiefung des Art. 8 Abs. 2 S. 2 GRCh, wodurch der betroffenen Person ausdrücklich das Recht gegeben werden soll, zu überprüfen, ob deren personenbezogenen Daten rechtmäßig verarbeitet werden.[451] Sie kann also von einem Verantwortlichen verlangen, Bestätigung und Auskunft über die Verarbeitung von sie betreffenden personenbezogenen Daten zu erhalten. Dabei soll es der betroffenen Person so einfach wie nur möglich gemacht werden. Gegenüber der bisherigen Rechtslage erweitert Art. 15 DSGVO den Auskunftsgegenstand, macht die Auskunft im Normalfall kostenlos und gibt der betroffenen Person das Recht, eine Kopie ihrer vorhandenen Daten zu erhalten.[452] Dieses Recht ist Grundlage und zentrales Element für die Ausübung der weiteren Betroffenenrechte der DSGVO, denn nur mit der Auskunft kann die betroffene Person überprüfen, ob die Verarbeitung rechtmäßig ist und das notwendige Wissen erlangen, um entsprechend Gebrauch bspw. vom Recht auf Löschung oder Berichtigung zu machen.[453]

Für eine rechtmäßige Auskunftserteilung ist lediglich ein Begehren der betroffenen Person gegenüber dem Verantwortlichen notwendig, sodass die sog. Holschuld bei der betroffenen Person liegt.[454] Dabei ist es völlig gleichgültig, in welcher Form dieses Begehren kundgetan wird und ob der Antragssteller geschäftsfähig ist.[455] Im Umkehrschluss bedeutet dies natürlich auch, dass der Verantwortliche die Auskunft nicht von sich aus

451 *Albrecht/Jotzo,* Das neue Datenschutzrecht der EU, 2017, Teil 4 Rn. 9.
452 *Stollhoff* (2020), Art. 15 Rn. 2 ff.
453 *Mester* (2019), Art. 15 Rn. 1.
454 *Dix* (2019), Art. 15 Rn. 3.
455 *Specht* (2018), Art. 15 Rn. 25.

zur Verfügung stellen muss, sondern einen Antrag einer betroffenen Person abwarten kann.[456]

Ob der Verantwortliche überhaupt personenbezogene Daten zum Antragsteller vorliegen hat, spielt keine Rolle bezüglich des Anspruchs auf Auskunft. Vielmehr ist die Frage nach Vorhandensein von personenbezogenen Daten Teil der Auskunft und kann vom Verantwortlichen entsprechend mit einer Negativauskunft beantwortet werden.[457] Aus diesem Grund differenziert Art. 15 Abs. 1 DSGVO bewusst zwischen der Bestätigung, ob betreffende personenbezogene Daten verarbeitet werden und der Auskunft an sich. Auch dies stärkt die Position der betroffenen Person, da das Recht auf Auskunft demnach voraussetzungslos ist[458] und Anfragen auch aufgrund von bloßen Vermutungen rechtmäßig sind und vom Verantwortlichen beantwortet werden müssen.[459]

Bei Eingang eines solchen form- und voraussetzungslosen Antrags bei einem Verantwortlichen und um zu verhindern, dass personenbezogene Daten einer Person fälschlicherweise an einen Dritten übermittelt werden,[460] sollen Verantwortliche gemäß ErwG 64 alle vertretbaren Mittel nutzen, um die Identität der antragsstellenden Person zu bestätigen. Aus Erwägungsgrund 64 ergibt sich aber auch, dass personenbezogene Daten durch den Verantwortlichen nicht nur mit dem Zweck gespeichert werden dürfen, auf mögliche Auskunftsersuche reagieren zu können. Nur, wenn der Verantwortliche begründete Zweifel an der Identität des Antragstellers hat, kann er gemäß Art. 12 Abs. 6 DSGVO weitere Informationen anfordern, welche die Identifizierung der betroffenen Person gewährleisten.

II. Auskunftsumfang

Vom Auskunftsanspruch sind grundsätzlich alle verarbeiteten Daten betroffen, die zur jeweiligen betroffenen Person vorhanden sind.[461] Im Umkehrschluss bedeutet dies, dass Daten, die der Verantwortliche in der Vergan-

456 *Franzen* (2018), Art. 15 DSGVO Rn. 4.
457 *Franck* (2018), Art. 15 Rn. 5.
458 *Mester* (2019), Art. 15 Rn. 2.
459 Anderer Meinung: *Specht* (2018), Art. 15 Rn. 5 mit Verweis auf Urteil zu § 34 BDSG a.F.: Hess LAG, Urt. v. 29.01.2013 – 13 Sa 263/12, Zeitschrift für Datenschutz 2013, 413.
460 *Nink* (2019), Art. 15 Rn. 10.
461 *Mester* (2019), Art. 15 Rn. 3.

genheit einmal verarbeitet hat, aber über die er beim Zeitpunkt des Antrags nicht mehr verfügt, nicht vom Auskunftsrecht betroffen sind.[462] Das Auskunftsrecht erstreckt sich vollumfänglich auf alle bei Antragsstellung vorliegenden Daten zur betroffenen Person, sodass eine Löschung der Daten bei Antragseingang oder eine Reduzierung der Auskunft auf die seit dem letzten Auskunftsantrag hinzugekommenen Daten nicht rechtmäßig sind.[463] Die Informationen, die von der Auskunft betroffen sind, zählt Art. 15 Abs. 1 DSGVO abschließend auf.[464] Der betroffenen Person muss demnach mitgeteilt werden, zu welchem Zweck die Daten verarbeitet werden, welche Kategorien von personenbezogenen Daten betroffen sind, an welche Empfänger oder Kategorien von Empfängern die Daten übermittelt werden, die Speicherdauer, welche Betroffenenrechte bestehen, woher die Daten kommen, ob eine automatisierte Entscheidungsfindung eingesetzt wird und welche geeigneten Garantien vorliegen, falls die Daten in ein Drittland übermittelt werden. Für den Fall der Verarbeitung von Wesensdaten durch BCI ist besonders die Mitteilung über die automatisierte Entscheidungsfindung relevant.

Sollte der Verantwortliche von automatisierter Entscheidungsfindung, einschließlich Profiling, i.S.v. Art. 22 Abs. 1 und 4 DSGVO Gebrauch machen, muss er dies im Zuge der Auskunft gemäß Art. 15 Abs. 1 lit. h DSGVO der betroffenen Person kundtun. Unter automatisierter Entscheidungsfindung sind alle Datenverarbeitungen zu verstehen, die ohne jegliches beeinflussendes menschliches Einwirken stattfinden und mit denen Entscheidungen gefällt werden.[465] Profiling wiederum ist in Art. 4 S. 4 DSGVO legaldefiniert. Es handelt sich demnach um jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Dem Wortlaut entsprechend müssen mindestens in den Fällen des Art. 22 Abs. 1 und 4 DSGVO aussagekräftige Informationen über die invol-

462 Ebenda.
463 *Bäcker* (2020), Art. 15 Rn. 8.
464 *Stollhoff* (2020), Art. 15 Rn. 13.
465 *Spindler/Horváth* (2019), Art. 22 Rn. 5.

vierte Logik sowie über die Folgen für die betroffene Person mitgeteilt werden. „Mindestens in den Fällen" verdeutlicht, dass diese Auskunftspflicht auf jeden Fall bei den automatisierten Entscheidungsfindungen nach Art. 22 Abs. 1 und 4 DSGVO gilt, aber auch auf eventuelle weitere automatisierte Entscheidungsfindungen nach Ermessen des Verantwortlichen angewendet werden kann.[466]

Aufgrund der ungenauen Formulierungen „aussagekräftige Informationen" und „involvierte Logik" entstehen jedoch Auslegungsspielräume.[467] Es kann nichtsdestotrotz festgehalten werden, dass mit der „involvierten Logik" nicht die Offenlegung des mathematischen Algorithmus des Verfahrens gemeint ist, da dies schließlich Betriebs- und Geschäftsgeheimnisse gefährden würde.[468] Erwägungsgrund 63 S. 5 unterstreicht diese Annahme, indem erläutert wird, dass das Recht des Geschäftsgeheimnisses nicht beeinträchtigt werden soll. Relevante aussagekräftige Informationen zur involvierten Logik sind demnach vielmehr die Grundannahmen des Algorithmus,[469] also welche Daten in die Berechnung einfließen, die Methodik der Berechnung und welche Auswirkungen die Ergebnisse haben könnten. Ebenso müssen in diesem Fall der Auskunftserteilung bereits vorhandene Auswertungen sowie darauf beruhende Entscheidungen mitgeteilt werden.[470] So müsste bspw. mitgeteilt werden, wenn aufgrund schlechterer Bonität die Kreditwürdigkeit abgestuft wurde.[471]

III. Recht auf Datenkopie

Eine interessante Neuerung im Zuge der DSGVO und einen wesentlichen Bestandteil des Auskunftsrechts stellt Art. 15 Abs. 3 S. 1 DSGVO dar, wonach der Verantwortliche dazu verpflichtet ist, eine Kopie der personenbezogenen Daten zur Verfügung zu stellen. Dem Wortlaut entsprechend, ist die Kopie nur auf die Daten zu beschränken, die tatsächlich Gegenstand der Verarbeitung sind[472] und die sich tatsächlich auf die betroffene Person beziehen, sodass ggf. vorhandene Daten Dritter unkenntlich gemacht wer-

466 *Kamlah* (2018), Art. 13 Rn. 28.
467 *Schmidt-Wudy* (2020), Art. 15 Rn. 78.
468 *Roßnagel/Nebel/Richter,* Zeitschrift für Datenschutz 2015, S. 455 (458).
469 *Paal/Hennemann* (2021), Art. 13 Rn. 31c.
470 *Bäcker* (2020), Art. 15 Rn. 27.
471 *Paal/Hennemann* (2021), Art. 13 Rn. 31a.
472 *Kamlah* (2018), Art. 15 Rn. 16.

den müssen.[473] Ebenso schreibt Art. 15 Abs. 4 DSGVO vor, dass durch die Kopie der Daten keine Rechte und Freiheiten anderer Personen beeinträchtigt werden dürfen. Diesbezüglich muss das Datenschutzrecht anderer Personen ebenso gewahrt werden.[474] Zudem sind Rechte des Verantwortlichen unter die Rechte und Freiheiten anderer Personen zu subsumieren,[475] sodass Geschäftsgeheimnisse oder geistiges Eigentum nach Erwägungsgrund 63 zurecht als schutzwürdig gelten. Das Vorliegen eines schutzwürdigen Rechts einer anderen Person soll aber nicht dazu führen, dass gar keine Kopie ausgestellt wird.[476] Vielmehr muss dann eine Teilkopie der Daten ausgestellt werden, die bspw. um die Daten Dritter bereinigt wurde.[477] Datenbankstrukturen müssen nicht kopiert werden.[478] Die Daten sind in den meisten Fällen ohne weitere Aufbereitung zu übermitteln, da sonst eine Verfälschung der Daten oder des Aussagegehalts der Daten entstehen könnte.[479] Sollte die Komplexität der Daten jedoch für den durchschnittlichen Empfänger nicht mehr verständlich sein, ist eine Aufbereitung der Daten durchaus sinnvoll. Dabei ist zu beachten, dass bei der Aufbereitung nicht der ursprüngliche Aussagegehalt verfälscht wird. Ansonsten wird der Zweck der Auskunft, der betroffenen Person einen Überblick zu verschaffen, verfehlt. Bei der Kopie der Daten geht es schließlich darum, dass der betroffenen Person ergänzend zu den allgemeinen Informationen aus Art. 15 Abs. 1 und 2 DSGVO, ein genauer Einblick gewährt wird, der die Prüfung der Rechtmäßigkeit der Verarbeitung ermöglicht.[480] Eine solche Prüfung ist aber nicht möglich, wenn der Empfänger die Datensätze nicht verstehen und interpretieren kann.

Eine Kopie ist dabei eine Verkörperung der Daten in einer einheitlichen Form.[481] Welche Form dies genau ist, wird nicht definiert.[482] Gemäß Art. 15 Abs. 3 S. 3 DSGVO ist jedoch ein gängiges elektronisches Format gestattet, und zwar besonders dann, wenn die betroffene Person den Auskunftsantrag bereits elektronisch gestellt hat. Ein gängiges elektronisches Format

473 *Bäcker* (2020), Art. 15 Rn. 42.
474 *Franck* (2018), Art. 15 Rn. 34.
475 *Bäcker* (2020), Art. 15 Rn. 42.
476 *Franck* (2018), Art. 15 Rn. 34.
477 *Bäcker* (2020), Art. 15 Rn. 42a.
478 *Kamlah* (2018), Art. 15 Rn. 16.
479 *Mester* (2019), Art. 15 Rn. 19.
480 *Schwartmann/Klein* (2018), Art. 15 Rn. 34.
481 *Franck* (2018), Art. 15 Rn. 28.
482 *Kamlah* (2018), Art. 15 Rn. 16.

ist dabei nicht als interoperable Kopie zu verstehen,[483] sondern als weitverbreitetes und verkehrsübliches Format wie bspw. PDF oder Microsoft Office Dateien.[484] Denkbar ist auch die Herausgabe der Daten auf einem Datenträger[485] oder aber per Fernzugang zu einem sicheren System, das der betroffenen Person direkten Zugang zu ihren Daten ermöglichen soll, wie es Erwägungsgrund 63 S. 4 nach Möglichkeit nahelegt. Der Fernzugriff ist dabei als Alternative zu Datenträgern oder elektronischen Formaten zu verstehen.[486]

Die Herausgabe der ersten Datenkopie muss unentgeltlich geschehen.[487] Sollte die betroffene Person darüber hinaus noch weitere Kopien anfordern, kann der Verantwortliche gemäß Art. 15 Abs. 3 S. 2 DSGVO pro Kopie ein angemessenes Entgelt auf Grundlage der Verwaltungskosten erheben. Damit ein Entgelt seitens des Verantwortlichen erhoben werden darf, muss die angeforderte Kopie keine signifikante Änderung zu der letzten ausgehändigten Kopie aufweisen.[488] Ansonsten kann davon ausgegangen werden, dass ein angemessener Zeitraum zwischen den jeweiligen Datenkopien liegt, sodass erneut Kostenfreiheit gilt.[489] Parallel dazu greift auch Art. 12 Abs. 5 S. 2 DSGVO.

IV. Das Auskunftsrecht bei BCI

1. Automatisierte Entscheidungsfindung

Bei der Datenverarbeitung mittels BCI könnte eine automatisierte Entscheidungsfindung vorliegen. Dies wird wahrscheinlich immer dann der Fall sein, wenn ein grundsätzliches Monitoring und Auswerten von Gehirnaktivitäten vorliegen. Die Aufzeichnung, Extraktion und Übersetzung der relevanten Gehirnsignale sowie die Generierung des jeweiligen Outputs, bzw. das Treffen jeweiliger Entscheidungen, kann vollständig ohne menschliches Einwirken stattfinden. Auch kann ein BCI genutzt werden, um eine große Menge von Wesensdaten zu verarbeiten, welche gut dafür

483 *Paal* (2021), Art. 15 Rn. 36.
484 *Stollhoff* (2020), Art. 15 Rn. 31.
485 *Franck* (2018), Art. 15 Rn. 28.
486 Ebenda.
487 *Kamlah* (2018), Art. 15 Rn. 17.
488 *Mester* (2019), Art. 15 Rn. 22.
489 *Franck* (2018), Art. 15 Rn. 32.

geeignet sind, um persönliche Aspekte einer Person zu bewerten, analysieren oder vorherzusagen.

Es kann somit oftmals geboten sein, dass Verantwortliche bei einem Auskunftsersuch aussagekräftige Informationen über die involvierte Logik sowie über die Folgen für die betroffene Person mitteilen. Dies könnte bei EEG-BCI folgendermaßen aussehen:

„Ihr Brain-Computer Interface zeichnet ihre Gehirnaktivitäten auf. Dies ist möglich, da Ihr Gehirn elektronische Signale erzeugt, die mittels eines EEGs beobachtet werden können. Diese aufgezeichneten neurologischen Aktivitäten werden automatisch so aufbereitet, dass nur noch relevante Signale vorhanden sind. Diese relevanten Signale werden dann mittels eines Algorithmus in Outputs übersetzt. Der eingesetzte Algorithmus ist dazu in der Lage, da dieser mit etlichen neurologischen Aktivitäten trainiert wurde und gelernt hat, welche Gehirnsignale für welche Outputs stehen. Die Entscheidungen, die vollautomatisiert durch den Algorithmus getroffen werden, betreffen somit z.B. die konkrete Bewegung Ihres Hilfsroboters o.Ä."[490]

In anderen Fällen kann allerdings auch davon ausgegangen werden, dass keine automatisierte Entscheidungsfindung vorliegt. Bei einer anlassbezogenen Verarbeitung von Wesensdaten mittels BCI, z.B. bei der gezielten Steuerung von Hilfsrobotern o.Ä., bedarf es schließlich eines initiierenden menschlichen Inputs, der die letztendliche Entscheidung/den Output vorgibt. Demnach findet zwar die konkrete Verarbeitung des Inputs automatisiert und ohne menschliches Einwirken statt, allerdings wird das Ergebnis der Verarbeitung bereits durch den menschlichen neurologischen Befehl vorgegeben. Dieser Ablauf ist mit dem bei Sprachassistenten vergleichbar. Dort wird ebenso ein menschlicher Input per Sprachbefehl gegeben, der dann völlig automatisiert aufgezeichnet, ausgewertet und in einen Output umgewandelt wird. Bei diesen bereits gängigen Verfahren wird allgemein auch nicht von automatisierter Entscheidungsfindung ausgegangen. Demnach gilt dasselbe analog für entsprechende Verarbeitungen durch BCI.

490 Geht davon aus, dass die Technologie und Verarbeitung zu komplex sind, um sinnvoll heruntergebrochen zu werden: *Greenberg,* Journal of Science and Technology 2019, S. 79 (109 ff.).

2. Datenkopie

Eine Übermittlung der Daten ohne weitere Aufbereitung ist bei einer Verarbeitung mittels BCI eher ungeeignet. Die Komplexität der Verarbeitung hätte zur Folge, dass die durchschnittliche betroffene Person nicht verstehen würde, welche Daten genau von ihr verarbeitet werden, wodurch es ihr unnötig erschwert werden würde, die Rechtmäßigkeit zu beurteilen. Demnach sollten die Daten strukturiert und erklärt werden.[491] Vor allem sollte der Verantwortliche den Zeitpunkt der Verarbeitung, eine Transkription/Beschreibung der neurologischen Signale, die damit erzeugten Outputs/Auswertungen/Ergebnisse sowie den dazugehörigen Dateinamen angeben. In den ergänzenden Dateien müssten dann die jeweiligen elektronischen Signale oder auch die nachmodellierten visuellen Reize als Darstellung hinterlegt sein. Eine Aufbereitung der Daten könnte also wie folgt aussehen:

Timestamp (UTC)	**Transkription/ Beschreibung**	**Output/ Auswertung/ Ergebnis**	**File**
2023-11-19, 21:01:23	links	Hilfsroboter bog links ab	2061a290d.pdf
2023-10-22, 11:45:33	Licht Küche an	Das Licht in der Küche wurde angeschaltet	2060a290e.pdf
2023-10-11	Ausschnitt einer Rede im Bundestag wurde gelesen/ gesehen	Zustimmung mit Rede wurde erkannt	2059a289c.pdf

Eine weitere wichtige Voraussetzung für eine DSGVO-konforme Datenkopie ist, dass nur die Daten der betroffenen Person bei der Auskunft übermittelt werden dürfen. Falls Daten Dritter vorhanden sind, müssen diese unkenntlich gemacht werden,[492] besonders da Art. 15 Abs. 4 DSGVO vorschreibt, dass die Rechte und Freiheiten anderer Personen nicht durch die Datenkopie beeinträchtigt werden dürfen. Dies könnte, je nach Einsatz der BCI, eine Herausforderung für Verantwortliche werden. Schließlich können visuelle Reize, also z.B. gesehene Gesichter, anhand von Gehirnaktivitäten mit hoher Übereinstimmung nachmodelliert werden.[493] Dies

491 Gleicher Meinung: *Greenberg,* Journal of Science and Technology 2019, S. 79 (109).
492 *Bäcker* (2020), Art. 15 Rn. 42.
493 *Nemrodov et al.,* eNeuro 2018, S. 1 (4 ff.).

geht so weit, dass gesehene Gesichter auch später noch rudimentär aus dem Gedächtnis der Nutzer ausgelesen werden können.[494] In diesen Fällen würden eindeutig Daten Dritter vorliegen, wenn auch ggf. in sehr abstrakter Form. Allerdings ist es fraglich, wie Verantwortliche in Zukunft sicherstellen sollen, dass diese Daten aus der Datenkopie entfernt werden. Sobald visuelle Reize grundsätzlich aus Gehirnaktivitäten ausgelesen werden, wird die Unterscheidung zwischen gewöhnlichen Daten und Daten einer dritten Person kaum realisierbar, ohne dass etliche Mitarbeiter alle Aufzeichnungen manuell durchgehen. Darum soll hier für eine Interessenabwägung plädiert werden. Die Rechte und Freiheiten anderer Personen sollen, soweit es geht, geschützt werden. Denkbar wäre bspw., dass die Modellierungssoftware, sobald es Gesichter erkennt, diese nur rudimentär und grob nachbildet. Damit würde bspw. verhindert werden, dass betroffene Dritte direkt erkannt werden. Ein Missbrauch mittels Gesichtserkennung wäre damit auch ausgeschlossen. Mit diesen Maßnahmen würden die Rechte und Freiheit der betroffenen Dritten weitestgehend geschützt. Da eine weitergehende Sortierung der Aufzeichnungen/Auswertungen unverhältnismäßig, technisch kaum möglich und kostenintensiv wäre, muss also eine Abwägung zugunsten des Auskunftsrechts der betroffenen Person vorgenommen werden. Denn wenn aus diesem Grund das Auskunftsrecht verweigert wird, würde Art. 15 DSGVO obsolet werden.

494 *Lee/Kuhl,* The Journal of Neuroscience 2016, S. 6069 (6075 ff.).

I. Technischer und organisatorischer Datenschutz bei der Verarbeitung von Wesensdaten

In der vorausgegangenen Erarbeitung konnte bereits gezeigt werden, dass Wesensdaten zwar in den Reglungsbereich der DSGVO fallen, jedoch nicht zwangsläufig den besonderen Schutz des Art. 9 DSGVO genießen. Ebenso wurde dargelegt, welche Rechtsgrundlagen für die Verarbeitung von Wesensdaten herangezogen werden können, welche diesbezüglichen Probleme bei der Einwilligung und dem berechtigten Interesse bestehen und wie das Auskunftsrecht bei einer Verarbeitung von Wesensdaten in Zukunft aussehen könnte.

Neben diesen grundlegenden Einordnungen von BCI und deren Datenverarbeitung in den Regelungsbereich der DSGVO, ist vor allem die Betrachtung des technischen Datenschutzes bei dieser neuen Technologie zentral. Anschließend soll demnach dargelegt werden, wie die derzeitige Lage der Cybersicherheit in Deutschland und weltweit ist und welche konkreten Cybersicherheits-Bedrohungen bei BCI bestehen. Darauf aufbauend soll überprüft werden, wie sich die technischen und organisatorischen Maßnahmen aus Art. 32 DSGVO bei BCI gestalten könnten. Ebenso wird überprüft, ob der geforderte Datenschutz durch Technikgestaltung und die geforderten datenschutzfreundlichen Voreinstellungen aus Art. 25 DSGVO sinnvollerweise bei BCI Anwendung finden und wie eine solche Anwendung in Zukunft konkret aussehen könnte.

I. Die Relevanz von Datensicherheit bei BCI

1. Die Lage der Cybersicherheit

In einer weiterhin zunehmend digitalisierten Welt steigen auch die Cybersicherheitsbedrohungen. Dies zeigt sich besonders in den diesbezüglich erfassten Straftaten in Deutschland. Bis 2021 ist die Anzahl an Cybercrime-Fällen, die in Deutschland polizeilich erfasst wurden, kontinuierlich

gestiegen.[495] Nur wenige dieser Fälle konnten allerdings auch aufgeklärt werden.[496] Laut dem Bundesamt für Sicherheit in der Informationstechnik, steigen zudem die Meldungen bzgl. Cybercrime-Vorfällen in KRITIS-Sektoren stetig.[497] Auch weltweit lässt sich ein vergleichbarer Trend ausmachen.[498]

Privatpersonen geraten dabei derzeit vermehrt bei Phishing-Versuchen ins Visier und sind von Datenleaks betroffen.[499] Unternehmen wiederum haben häufiger mit Ransomware, Malware, Phishing und Passwortdiebstahl zu kämpfen.[500]

Motiv hinter den Attacken sind in den meisten Fällen finanzielle Interessen, wie eine Auswertung des US-amerikanischen Telekommunikationsdienstleisters Verizon nahelegt.[501] Dabei wird häufig von Erpressung Gebrauch gemacht, in dem bspw. Unternehmensdaten verschlüsselt werden und erst nach Zahlung einer geforderten Summe wieder entschlüsselt werden oder indem gedroht wird, dass bei Nichtzahlung eine Veröffentlichung von sensiblen Daten stattfindet.[502] Neben Erpressung werden Daten auch gestohlen und im Internet zum Kauf angeboten.[503] Die Käufer der Daten

---

495 *Bundeskriminalamt,* Bundeslagebild Cybercrime 2023, v. 13.5.2024, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=28110, S. 7 (abgerufen 4.1.2025).

496 *Ebenda.*

497 *Bundesamt für Sicherheit in der Informationstechnik,* Die Lage der IT-Sicherheit in Deutschland 2024, v. 12.11.2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5, S. 62 f. (abgerufen 4.1.2025); Abrufbar unter: https://de.statista.com/statistik/daten/studie/1230654/umfrage/anzahl-der-kritis-meldungen-an-das-bsi/ (abgerufen 4.12.2022).

498 Abrufbar unter: https://web.archive.org/web/20201129054027/https://zhenjess.github.io/Breach/ (abgerufen 4.12.2022).

499 *Bundesamt für Sicherheit in der Informationstechnik,* Die Lage der IT-Sicherheit in Deutschland 2024, v. 12.11.2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5, S. 56 f. (abgerufen 4.1.2025).

500 *Ebenda,* S. 61.

501 Abrufbar unter: https://www.verizon.com/business/resources/reports/dbir/2020/results-and-analysis/ (abgerufen 4.12.2022).

502 *Bundesamt für Sicherheit in der Informationstechnik,* Die Lage der IT-Sicherheit in Deutschland 2024, v. 12.11.2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5, S. 19 ff. (abgerufen 4.1.2025).

503 Übersicht von gängigen Preisen für verschiedene Datensätze: *Ruffio,* Dark Web Price Index 2022, v. 19.9.2022, https://www.privacyaffairs.com/dark-web-price-index-2022/ (abgerufen 4.12.2022).

können diese dann wiederum z.B. für Identitätsdiebstahl, Betrug oder Erpressung nutzen.

2. Cybersicherheit bei BCI

Im IT-Grundschutz-Kompendium identifiziert das Bundesamt für Sicherheit in der Informationstechnik, dass sich IT-Sicherheitsvorfälle entweder auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten und Systemen auswirken können.[504] Die DSGVO ergänzt diese Aufzählung in Art. 32 Abs. 1 lit. b DSGVO noch um die Belastbarkeit von Systemen.

In Anbetracht der derzeitigen Cybersecurity-Lage und dem informationsschöpfungspotential von BCI, ist es wahrscheinlich, dass BCI-Nutzer und -Anbieter in Zukunft vermehrt Ziel von Cyberangriffen sein könnten. Auch für BCI ergeben sich demnach konkrete Bedrohungsszenarien, die sich eben auf die Vertraulichkeit, Integrität, Verfügbarkeit oder Belastbarkeit auswirken können.

a. Vertraulichkeit

Wie bereits ausführlich dargelegt, werden durch BCI viele sensitive personenbezogene Daten verarbeitet. Diese sollten grundsätzlich nur der betroffenen Person und falls notwendig dem vertrauensvollen Anbieter zugänglich sein. Allerdings bieten sich auch bei BCI Möglichkeiten, dass die Technologie böswillig manipuliert oder ausgespäht wird, um Zugang zu oder Kenntnis von Daten zu erhalten. So zeigt eine Studie, dass es bereits mit einem gängigen EEG-Headset möglich ist, die Bankkarten PIN, das dazugehörige Bankinstitut, den geographischen Standort und den Geburtsmonat des Nutzers unbemerkt zu erhalten.[505] Dies gelang, indem die betroffene Person unbewusst visueller Stimuli ausgesetzt wurde, worauf eine neurologische Reaktion aufgezeichnet und entsprechend ausgewertet werden konnte. Auch wenn diese Methode vergleichsweise aufwändig ist, könnte sie in Zukunft dafür genutzt werden, um noch viel umfangreichere

504 Abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, S. 1 (abgerufen am 6.1.2025).

505 *Martinovic et al.,* Proceedings of the 21st USENIX Security Symposium 2012, S. 1 (5 ff.).

Daten von Personen zu erhalten.[506] Es könnte also eine Art „Brain-Spyware" entstehen, die nicht nur für Hacker mit finanziellen Absichten interessant wäre, sondern auch für Strafverfolgungsbehörden.[507]

Bei einem solchen unberechtigten Zugang zu Wesensdaten ergeben sich vielfältige mögliche Auswirkungen für die betroffenen Personen. Angreifer könnten diese bspw. mit sensiblen Daten erpressen, die Daten im Internet verkaufen oder auch dazu nutzen, um Identitätsdiebstahl und andere Betrugshandlungen durchzuführen.[508]

b. Integrität

Des Weiteren kann auch die Korrektheit von Informationen bei BCI böswillig manipuliert werden. Von einer solchen Manipulation könnten Daten, Kommunikation, Einstellungen und Befehle betroffen sein.[509] Ein Verlust der Integrität könnte demnach u.a. dazu führen, dass falsche Updates oder fehlerhafte Kommunikation eingespielt werden,[510] die Kontrolle über das Gerät übernommen wird[511] oder sogar eine Manipulation der neurologischen Abläufe stattfindet, um bspw. Emotionen oder Schmerzen zu beeinflussen.[512] Laut einiger Meinungen könnte dies in Zukunft so weit gehen, dass auch die Gedanken und entsprechende Handlungen einer betroffenen Person manipuliert werden könnten.[513]

---

506 *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (200 f.); Bsp.: Identifikation von unterbewusster Gesichtserkennung: *Vargas Martin/Cho/Aversano,* ACM Transactions on Applied Perception 2016, Article 7 S. 1 (10 f.).

507 *Bonaci/Calo/Chizeck,* IEEE Technology and Society Magazine 2015, S. 32 (35 f.); *Farahany,* Stanford Law Review 2011, S. 11 (11 ff.).

508 *Browning/Tuma,* South Carolina Law Review 2016, S. 637 (661); *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (201 f.)

509 *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (202); *Browning/Tuma,* South Carolina Law Review 2016, S. 637 (644 ff.); *Gasson/Koops,* Law, Innovation and Technology 2013, S. 248 (264); *Denning/Matsuoka/Kohno,* Journal of Neurosurgery 2009, S. 1 (2); *Bernal et al.,* ACM Computing Surveys 2022, S. 1 (10 ff).

510 *Bernal et al.,* ACM Computing Surveys 2022, S. 1 (10 ff); *Gasson/Koops,* Law, Innovation and Technology 2013, S. 248 (265); *Denning/Matsuoka/Kohno,* Journal of Neurosurgery 2009, S. 1 (3).

511 *Pycroft et al.,* World Neurosurgery 2016, S. 454 (454 ff.).

512 *Denning/Matsuoka/Kohno,* Journal of Neurosurgery 2009, S. 1 (3); *Gasson/Koops,* Law, Innovation and Technology 2013, S. 248 (266);

513 *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (202).

c. Verfügbarkeit und Belastbarkeit

Damit ein BCI funktionsfähig bleibt, muss abschließend auch die Verfügbarkeit und Belastbarkeit des Systems gewährleistet werden. Sobald diese nicht mehr gewährleistet werden kann, könnte dies für die Nutzer schwere Auswirkungen haben. So könnten bspw. per BCI kontrollierte Prothesen oder Hilfsroboter nicht mehr gesteuert werden.[514]

Eine diesbezügliche Bedrohung stellen besonders sog. DoS (Denial-of-Service)- und DDoS (Distributed-Denial-of-Service)-Angriffe dar. Dabei wird ein System mit einem übermäßig hohen Volumen von Anfragen überlastet, womit die Umsetzung von legitimen Anfragen verhindert wird.[515] Das gefährliche an DDoS-Attacken ist dabei, dass die Anfragen von einer Vielzahl von Quellen kommen.[516] Während bei einem DoS-Angriff also die Quelle identifiziert und blockiert werden kann, muss bei einer DDoS-Attacke häufig das System komplett vom Netzwerk genommen werden. Auf die Belastbarkeit wirken sich solche Angriffe dann aus, wenn eine Beeinträchtigung der Funktionsfähigkeit nicht schnell wiederhergestellt werden.[517]

II. Art. 32 DSGVO: Technische und organisatorische Maßnahmen

1. Zweck und Inhalt der Reglung

Um der vorausgehend beschriebenen Cybersicherheits-Lage gerecht zu werden, verlangt die DSGVO technische und organisatorische Maßnahmen von Verantwortlichen, um die Sicherheit der verarbeiteten personenbezogenen Daten zu gewährleisten. Art. 32 DSGVO nimmt dabei eine globale Sicht in Bezug auf den Datenschutz ein.[518] Art. 32 DSGVO fordert somit einen generellen Schutz von personenbezogenen Daten, sobald diese von einem Verantwortlichen verarbeitet werden.[519] Es wird der Datensicherheits-Grundsatz aus Art. 5 Abs. 1 lit. f DSGVO aufgegriffen und konkretisiert, womit die gesetzliche Idee des individuellen Datenschutzes um die

514 *Denning/Matsuoka/Kohno,* Journal of Neurosurgery 2009, S. 1 (3).
515 *Hellmann,* IT-Sicherheit, 2018, S. 113; *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (202).
516 *Hellmann,* IT-Sicherheit, 2018, S. 113.
517 *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (202).
518 *Martini* (2021), Art. 32 Rn. 1 f.; *Jandt* (2020), Art. 32 Rn. 1 f.
519 *Wolff* (2017), Rn. 843.

eher allgemeingültige und technisch orientierte Datensicherheit ergänzt wird und vice versa.[520]

2. Auswahlkriterien für geeignete Maßnahmen

Laut Art. 32 Abs. 1 DSGVO sollen der Verantwortliche sowie involvierte Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen, um ein angemessenes Schutzniveau bei der jeweiligen Verarbeitung von personenbezogenen Daten zu gewährleisten. Zentral ist demnach die Risikovermeidung, die sicherstellen soll, dass personenbezogene Daten nicht rechtswidrig verarbeitet werden.[521] Technische Maßnahmen beziehen sich dabei auf die technischen Hilfsmittel, die bei der Verarbeitung Anwendung finden, wohingegen organisatorische Maßnahmen die Umstände der Datenverarbeitung betreffen.[522] Ab wann eine Maßnahme geeignet ist, definiert die DSGVO dabei nicht. Dies bietet den Vorteil, dass Verantwortliche individuell festlegen können, welche Maßnahmen notwendig sind, um einen angemessenen Schutz zu gewährleisten, ohne, dass diese aufgrund von festgelegten Maßnahmen eingeschränkt oder aber mit einem unverhältnismäßigen Aufwand konfrontiert werden.[523] Damit eine Maßnahme geeignet ist, ist es somit grundsätzlich notwendig, dass diese der Eindämmung des Risikos der Datenverarbeitung dienlich sind[524] und vor allem die Grundsätze aus Art. 5 DSGVO, mit einem Fokus auf die Integrität und Vertraulichkeit der Datenverarbeitung, berücksichtigen.[525] Bei der Auswahl dieser geeigneten Maßnahmen sollen der Stand der Technik, die Implementierungskosten, die Art, der Umfang, der Umstand und der Zweck der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schweren des Risikos für die Rechte und Freiheiten der Betroffenen berücksichtigt werden. Die Vorgaben sind bereits bei der initialen Planung einer Datenverarbeitung zu berücksichtigen und sollen den kompletten Lebenszyklus der Daten (inkl. Löschung) berücksichtigen.[526]

520 *Martini* (2021), Art. 32 Rn. 1b; *Wolff* (2017), Rn. 844; *Hansen* (2019), Art. 32 Rn. 12.
521 *Jandt* (2020), Art. 32 Rn. 5; *Schultze-Melling* (2022), 4. Aufl., Art. 32 Rn. 2.
522 *Martini* (2021), Art. 25 Rn. 21 f.
523 *Hladjk* (2018), Art. 32 Rn. 4.
524 *Jandt* (2020), Art. 32 Rn. 5.
525 *Martini* (2021), Art. 32 Rn. 2.
526 *Jandt* (2020), Art. 32 Rn. 6.

a. Stand der Technik

Um eine langfristige und nachhaltige Sicherheit bei der Datenverarbeitung zu gewährleisten, müssen Verantwortliche bei der Auswahl der Maßnahmen den Stand der Technik berücksichtigen. Das bedeutet, dass die ausgewählten Maßnahmen regelmäßig überprüft und ggf. angepasst werden müssen, sobald diese veraltet sind.[527] „Stand der Technik" bedeutet dabei auch, dass eine technische Möglichkeit für den Verantwortlichen vorliegen muss.[528] Diese umfasst dabei bekannte, bewährte und am Markt erhältliche Technologien[529] aber auch marktfähige Technologien, die sich schon bewiesen, aber noch nicht weitläufig durchgesetzt haben.[530]

b. Implementierungskosten

Um eine zu hohe wirtschaftliche Belastung für den Verantwortlichen zu vermeiden, soll auch der finanzielle Aufwand bei der Implementierung der Maßnahmen Berücksichtigung finden.[531] Dem Verantwortlichen obliegt es demnach, eine Kosten-Nutzen-Analyse durchzuführen, um festzustellen, ob die ggf. kostenintensive Maßnahme auch wirklich zur Eindämmung des Risikos beitragen kann.[532] Grundsätzlich gilt dabei: Je höher das Risiko der Verarbeitung, umso höhere Kosten können dem Verantwortlichen zugemutet werden.[533] Der finanzielle Aufwand ist dabei langfristig zu verstehen und umfasst somit nicht nur initiale Installationskosten o.Ä., sondern auch Folgekosten wie bspw. Wartungs- oder Servicekosten.[534]

527 *Hladjk* (2018), Art. 32 Rn. 5.
528 *Martini* (2021), Art. 32 Rn. 56a.
529 *Piltz* (2018), Art. 32 Rn. 18.
530 *Hladjk* (2018), Art. 32 Rn. 5; *Jandt* (2020), Art. 32 Rn. 10.
531 *Piltz* (2018), Art. 32 Rn. 21; *Martini* (2021), Art. 32 Rn. 60.
532 *Schultze-Melling* (2022), 4. Aufl., Art. 32 Rn. 14.
533 *Jandt* (2020), Art. 32 Rn. 11.
534 *Hansen* (2019), Art. 32 Rn. 26; *Martini* (2021), Art. 32 Rn. 60a; *Jandt* (2020), Art. 32 Rn. 11.

c. Art, Umfang, Umstand und Zweck der Verarbeitung

Um die zu gewährleistende Datensicherheit zu definieren, ist auf die relevanten Kriterien der Datenverarbeitung abzustellen.[535] Diese Kriterien sind die Art, der Umfang, der Umstand und der Zweck der Datenverarbeitung, woraus sich dann entsprechende technische und organisatorische Maßnahmen ableiten lassen sollen.

Die Art der Datenverarbeitung greift auf Art. 4 Nr. 2 DSGVO zurück, in dem vor allem das Erheben, Erfassen, die Übermittlung, das Ordnen, die Speicherung, das Löschen und die Vernichtung von Daten genannt werden.[536] Daneben ist ebenso miteinzubeziehen, welche Daten verarbeitet werden, also ob es sich um personenbezogene Daten handelt, die auf Grundlage von Art. 6 DSGVO verarbeitet werden oder um besondere Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO.[537]

Der Umfang der Verarbeitung wiederum bezieht sich auf die Quantität der betroffenen Personen, Daten und der damit einhergehenden Verarbeitung.[538] Dabei sind auch jene Daten zu berücksichtigen, die nicht zwangsläufig zentraler Bestandteil der Datenverarbeitung sind, aber nichtsdestotrotz ebenso verarbeitet werden (z.B. Logdateien).[539]

Umstände der Verarbeitung beschreiben die konkrete Umsetzung der Datenverarbeitung und beinhalten somit Aspekte wie z.B. wie die Daten erhoben werden, welche Verarbeitungsschritte durchgeführt werden, die Ausgestaltung der zugrundeliegenden technischen Infrastruktur sowie die Dauer der Verarbeitung insb. der Speicherung.[540]

Als abschließendes Kriterium findet auch der Verarbeitungszweck Berücksichtigung. Laut Art. 5 Abs. 1 lit. b gilt grundsätzlich, dass der Zweck einer Datenverarbeitung hinreichend bestimmt[541] und rechtmäßig sein muss.[542] Den konkreten Verarbeitungszweck kann der Verantwortliche selbstbestimmt festlegen.[543] Je invasiver und weitreichender der gewählte

535 *Hansen* (2019), Art. 24 Rn. 12.
536 *Martini* (2021), Art. 24 Rn. 32; *Jandt* (2020), Art. 32 Rn. 12.
537 *Hansen* (2019), Art. 32 Rn. 27; *Jandt* (2020), Art. 32 Rn. 12.
538 *Jandt* (2020), Art. 32 Rn. 12; *Martini* (2021), Art. 24 Rn. 33.
539 *Jandt* (2020), Art. 32 Rn. 12.
540 *Jandt* (2020), Art. 32 Rn. 12; *Martini* (2021), Art. 24 Rn. 34a.
541 *Reimer* (2018), Art. 5 Rn. 21.
542 *Herbst* (2020), Art. 5 Rn. 37.
543 *Martini* (2021), Art. 24 Rn. 35.

Verarbeitungszweck ist, umso schwerer sind allerdings auch die damit einhergehenden Risiken einzustufen.[544]

d. Eintrittswahrscheinlichkeit und Schwere des Risikos

Als letztes Auswahlkriterium für geeignete technische und organisatorische Maßnahmen wird die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen aufgeführt. Die Einstufung der Eintrittswahrscheinlichkeit kann auf Grundlage von statistischen Erfahrungswerten oder auch auf Grundlage von elaborierten Wahrscheinlichkeitsschätzungen vorgenommen werden.[545] Die Schadensschwere wiederum muss eingeschätzt werden, indem alle möglichen materiellen als auch immateriellen Schäden für betroffene Personen berücksichtigt werden[546] und deren jeweiliges Ausmaß. Hier könnte bspw. gemäß ErwG. 75 und 85 Kontrollverlust über Daten, Diskriminierung, Identitätsdiebstahl und Rufschädigung relevant sein. Welche Schadensszenarien und daraus resultierende Schadensschwere genau vorliegen, ist abhängig von Art, Umfang, Umstand und Zweck der Verarbeitung. Auch hier gilt grundsätzlich, dass eine Verarbeitung von besonderen Kategorien von personenbezogenen Daten tendenziell zu einer höheren möglichen Schadensschwere führt.[547] Je höher die Eintrittswahrscheinlichkeit und die mögliche Schadensschwere ist, umso höher muss dann auch das Schutzniveau sein.[548]

3. Geeignete Maßnahmen

Nach der Darlegung der Auswahlkriterien werden vom Gesetzgeber in Art. 32 Abs. 1 lit. a – d DSGVO ergänzend einige geeignete technische und organisatorische Maßnahmen genannt. Mit der Formulierung „unter anderem" wird angezeigt, dass diese Aufzählung nicht abschließend, sondern lediglich exemplarisch ist. Ebenso wird damit klargestellt, dass die Maßnah-

544 Ebenda.
545 *Martini* (2021), Art. 24 Rn. 30; *Jandt* (2020), Art. 32 Rn. 13.
546 *Jandt* (2020), Art. 32 Rn. 13; *Martini* (2021), Art. 24 Rn. 29.
547 *Martini* (2021), Art. 32 Rn. 52.
548 Nur in Bezug auf Eintrittswahrscheinlichkeit: *Martini* (2021), Art. 32 Rn. 51a.

men nicht verpflichtend sind, sondern nur als Vorschlag fungieren, der je nach Fall auf Geeignetheit überprüft werden muss.[549]

a. Pseudonymisierung und Verschlüsselung

Die erste der vorgeschlagenen Maßnahmen ist der Einsatz von Pseudonymisierung und Verschlüsselungen. Art. 4 Nr. 5 DSGVO enthält als Referenz eine Legaldefinition des Begriffs „Pseudonymisierung". Diese besagt, dass eben jene vorliegt, wenn personenbezogene Daten in einer Art und Weise verarbeitet werden, bei der es ohne Hinzuziehung von weiteren Informationen nicht mehr möglich ist, diese einer spezifischen betroffenen Person zuzuordnen. Dies wird dadurch gewährleistet, dass vorliegende Identifikationsmerkmale, wie z.B. ein Name, durch anderweitige Ziffern oder Kennzeichen ersetzt werden, welche nur mit einer entsprechenden Regel oder Zusatzinformation erneut der betroffenen Person zugeordnet werden können.[550] Dabei ist es geboten, die weiteren Informationen, die die betroffene Person identifizierbar machen könnte, gesondert aufzubewahren und zu schützen. Verschlüsselung bedeutet wiederum, dass die klare Lesbarkeit von Daten mithilfe von kryptografischen Mitteln so angepasst wird, dass die Daten nur noch mit dem richtigen Schlüssel auslesbar sind.[551] Damit soll sichergestellt werden, dass unbefugte Personen keinen Zugang zu personenbezogenen Daten erhalten.[552] Dies kann sowohl durch symmetrische (Kommunikationspartner besitzen denselben geheimen Schlüssel zum Ver- und Entschlüsseln)[553] als auch asymmetrische (Kommunikationspartner besitzen unterschiedliche Schlüssel zum Ver- und Entschlüsseln)[554] Verschlüsslungsverfahren geschehen.[555]

549 *Piltz* (2018), Art. 32 Rn. 24.
550 *Jandt* (2020), Art. 32 Rn. 18.
551 *Mantz* (2018), Art. 32 Rn. 11.
552 *Piltz* (2018), Art. 32 Rn. 28.
553 *Petrlic/Sorge,* Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, 2017, S. 15.
554 Ebenda, S. 16.
555 *Jandt* (2020), Art. 32 Rn. 19.

b. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

Mit dem Fokus auf Vertraulichkeit, Integrität und Verfügbarkeit werden die allgemeinen Schutzziele der IT-Sicherheit[556] vom Gesetzgeber aufgegriffen und um den Faktor der Belastbarkeit ergänzt.[557] Es wird empfohlen, die Schutzziele präventiv, über die gesamte Zeit der Datenverarbeitung hinweg und mit einer ganzheitlichen Betrachtungsweise des Datenverarbeitungssystems, zu verfolgen.[558] Das schließt auch regelmäßige Evaluierungen und (falls nötig) die Anpassung entsprechender Maßnahmen ein.[559]

Die Sicherstellung der Vertraulichkeit schützt vor unbefugter Kenntnisnahme von personenbezogenen Daten.[560] Dies wird vorgelagert bereits durch die Vertraulichkeit der Verarbeitungssysteme/-dienste gewährleistet.[561] Gängige Maßnahmen sind dabei die Implementierung von Berechtigungs- und Rollenkonzepten, der Einsatz von sicheren Authentifizierungsverfahren und auch die bereits betrachtete Verschlüsselung von personenbezogenen Daten.[562]

Die Sicherstellung der Integrität adressiert die Korrektheit der Daten.[563] Personenbezogene Daten und die eingesetzten Systeme sollen also vor unberechtigter Manipulation und Modifikation geschützt werden.[564] Um dies zu erreichen, können bspw. eingeschränkte Schreib- und Änderungsrechte zum Einsatz kommen, falsche Daten gelöscht oder berichtigt werden sowie elektronische Signaturen Anwendung finden.[565]

556 Abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, S. 1 (abgerufen am 6.1.2025).
557 *Jandt* (2020), Art. 32 Rn. 26.
558 *Hansen* (2019), Art. 32 Rn. 36 f.
559 *Hladjk* (2018), Art. 32 Rn. 8.
560 Abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, S. 1 (abgerufen am 6.1.2025).
561 *Jandt* (2020), Art. 32 Rn. 23.
562 Abrufbar unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf, S. 32 f. (abgerufen am 7.7.2022).
563 Abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, S. 1 (abgerufen am 6.1.2025).
564 *Martini* (2021), Art. 32 Rn. 36.
565 Abrufbar unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf, S. 32 (abgerufen am 7.7.2022).

Die Verfügbarkeit zielt darauf ab, dass die Nutzung von Systemen, Anwendungen sowie Informationen und Daten stets wie vorgesehen möglich ist.[566] Die Einhaltung dieses Schutzzieles ist bspw. durch Backups, redundante Systeme, die Erstellung von Notfallkonzepten und den Schutz vor Schadsoftware möglich.[567]

Die Belastbarkeit von Systemen und Diensten zielt ergänzend zu den klassischen Schutzzielen der IT-Sicherheit darauf ab, eine Resilienz zu erreichen, womit Störungen, die Einwirkung von Dritten oder sonstige widrige Umstände nicht mehr zwangläufig zu Ausfällen führen.[568] Auch soll die Sicherstellung der Belastbarkeit dazu führen, dass eine quantitativ und qualitativ übermäßige Inanspruchnahme des Systems bewältigt werden kann.[569] Als entsprechende Maßnahmen bieten sich hier redundante Systeme mit der Möglichkeit von load balancing,[570] die Verringerung von Angriffsflächen durch bspw. aktuelle Softwareversionen und die Einbindung von Intrusion-Detection-and-Response Systemen an.[571]

c. Wiederherstellbarkeit

Als weiteres Maßnahmenbündel schlägt die DSGVO in Art. 32 Abs. 1 lit. c DSGVO vor, dass die Wiederherstellbarkeit der Verfügbarkeit und des Zugangs zu personenbezogenen Daten nach einem physischen oder technischen Zwischenfall rasch gewährleistet werden sollte. Physische Zwischenfälle können dabei z.B. Wasserschäden, Brand oder Naturereignisse sein, die sich direkt auf die genutzte Hardware auswirken, wohingegen technische Zwischenfälle alle Komponenten des Systems betreffen können, weil z.B. Software fehlerhaft ausgeführt wird oder ein Angriff von außen vorliegt.[572] Eine Spezifizierung des zeitlichen Rahmens, in welchem die

566 *Piltz* (2018), Art. 32 Rn. 31; Abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, S. 1 (abgerufen am 6.1.2025).

567 Abrufbar unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf, S. 31 (abgerufen am 7.7.2022).

568 *Hansen* (2019), Art. 32 Rn. 42; *Martini* (2021), Art. 32 Rn. 39.

569 *Piltz* (2018), Art. 32 Rn. 31; *Hansen* (2019), Art. 32 Rn. 44; mit Verweis auf DoS-/DDoS-Attacken: *Martini* (2021), Art. 32 Rn. 39.

570 *Mantz* (2018), Art. 32 Rn. 17.

571 *Hansen* (2019), Art. 32 Rn. 45.

572 *Jandt* (2020), Art. 32 Rn. 27; *Hansen* (2019), Art. 32 Rn. 47.

Wiederherstellung durchgeführt werden sollte, findet nicht statt. Die Wortwahl „rasch" lässt allerdings darauf schließen, dass die zur Verfügung stehende Zeit länger ist, als bei der Notwendigkeit eines unverzüglichen Handelns.[573] Die Wiederherstellbarkeit der Daten kann dabei z.B. durch Backups, komplett gespiegelte Datenbanken oder Ausweichrechenzentren ermöglicht werden.[574]

d. Kontrollverfahren

Um den Maßnahmenkatalog abzurunden, schlägt die DSGVO abschließend regelmäßige Überprüfungen, Bewertungen und Evaluierungen der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vor. Damit wird ein mittelbares Instrument eingeführt, welches die Nachhaltigkeit der Datensicherheit in Abhängigkeit zum Stand der Technik und des vorhandenen Risikos gewährleisten soll.[575] Ebenso soll damit ein allgemeiner Nachweis erbracht werden können, dass die getroffenen Maßnahmen die Anforderungen des Art. 32 DSGVO erfüllen.[576] Als konkrete Maßnahmen wären dabei bspw. ein Penetrationstest, interne oder externe Audits oder ein Wiederanlauftest denkbar.[577] Die Regelmäßigkeit der Überprüfung sollte sich dabei grundsätzlich am vorhandenen Risiko oder an bestimmten Anlässen (z.B. neu bekannt gewordene Sicherheitslücken) orientieren.[578]

573 *Piltz* (2018), Art. 32 Rn. 33.
574 *Mantz* (2018), Art. 32 Rn. 18; *Jandt* (2020), Art. 32 Rn. 27; *Hansen* (2019), Art. 32 Rn. 51; *Martini* (2021), Art. 32 Rn. 41c.
575 *Hansen* (2019), Art. 32 Rn. 55; *Jandt* (2020), Art. 32 Rn. 29; *Mantz* (2018), Art. 32 Rn. 20.
576 *Piltz* (2018), Art. 32 Rn. 36.
577 *Martini* (2021), Art. 32 Rn. 44; *Mantz* (2018), Art. 32 Rn. 20; *Hansen* (2019), Art. 32 Rn. 56; *Jandt* (2020), Art. 32 Rn. 30.
578 *Mantz* (2018), Art. 32 Rn. 21; *Jandt* (2020), Art. 32 Rn. 30; *Martini* (2021), Art. 32 Rn. 45.

III. Art. 25 Abs. 1 DSGVO: Datenschutz durch Technikgestaltung

1. Zweck und Inhalt der Reglung

Während Art. 32 DSGVO eine globale Datensicherheit fordert, adressiert Art. 25 Abs. 1 DSGVO explizit den technischen Datenschutz bei der Auswahl, Konzeptionierung und Erstellung sowie bei der letztendlichen Nutzung eines Datenverarbeitungssystems. Art. 25 Abs. 1 DSGVO fordert demnach, dass bereits bei der initialen Festlegung der Mittel, die bei der Datenverarbeitung eingesetzt werden sollen, sowie bei der eigentlichen Verarbeitung, geeignete technische und organisatorische Maßnahmen implementiert werden müssen, die die Einhaltung aller Datenschutzgrundsätze aus Art. 5 DSGVO gewährleisten.[579] Dabei sollen laut Gesetzestext ebenso der Stand der Technik, die Implementierungskosten sowie die Art, der Umfang, die Umstände, der Zweck und die Risiken der Verarbeitung berücksichtigt werden. Damit soll erreicht werden, dass Datenschutz proaktiv bereits bei der Auswahl oder bei der Erstellung sowie Einrichtung von Verarbeitungssystem Berücksichtigung findet und nicht erst, wenn ein Verfahren bereits etabliert wurde.[580] Demnach müssen bereits bei dem Entwurf und der Programmierung von Datenverarbeitungsanwendungen, die datenschutzrechtlichen Grundprinzipien eingehalten werden.[581] Gleiches gilt beim Einkauf bzw. bei der Anmietung von entsprechenden Anwendungen.[582] Wie von Art. 25 Abs. 1 DSGVO gefordert, sind die geeigneten Maßnahmen nicht nur auf die Technik zu beschränken, sondern umfassen auch organisatorische Maßnahmen.[583]

2. Beispiele für Datenschutz durch Technikgestaltung

Für die Einhaltung der jeweiligen Datenschutzgrundsätze aus Art. 5 DSGVO durch Technikgestaltung bieten sich verschiedene Maßnahmen an. Als explizites Beispiel einer solchen Maßnahme nennt Art. 25 Abs. 1 DSGVO lediglich die Pseudonymisierung von personenbezogenen Daten.

579 *Hartung* (2020), Art. 25 Rn. 14; *Nolte/Werkmeister* (2018), Art. 25 Rn. 12.
580 *Baumgartner* (2018), Art. 25 Rn. 1; *Nolte/Werkmeister* (2018), Art. 25 Rn. 2; *Hartung* (2020), Art. 25 Rn. 11; *Hansen* (2019), Art. 25 Rn. 18; *Mantz* (2018), Art. 25 Rn. 2 ff.
581 *Hartung* (2020), Art. 25 Rn. 11; *Hansen* (2019), Art. 25 Rn. 18.
582 Ebenda.
583 *Nolte/Werkmeister* (2018), Art. 25 Rn. 17.

Weitere Beispiele können allerdings in Art. 24 sowie Art. 32 DSGVO gefunden werden, da die dort geforderten technischen und organisatorischen Maßnahmen als deckungsgleich zu verstehen sind.[584] Demnach ist z.B. auch die in Art. 32 DSGVO u.a. genannte Verschlüsselung sowie die Zugangs- und Zutrittskontrolle als valides Mittel für Datenschutz durch Technikgestaltung einsetzbar. Ebenso können die Anonymisierung von Daten,[585] die Kennzeichnung von Daten,[586] die Transparenz bei der Datenverarbeitung,[587] die Schulung von Mitarbeitern, die in der Datenverarbeitung tätig sind,[588] die Erstellung von Lösch- und Berechtigungskonzepten[589] und die Implementierung von sicheren Authentifizierungsmechanismen, wie z.B. Single-Sign-On-Services sinnvolle Maßnahmen sein, um Datenschutz durch Technikgestaltung zu gewährleisten.[590]

IV. Art. 25 Abs. 2 DSGVO: Datenschutz durch datenschutzfreundliche Voreinstellungen

1. Zweck und Inhalt der Reglung

Während Art. 25 Abs. 1 DSGVO die eigentliche technische Konzeption und Beschaffenheit von bspw. Software adressiert, zielt Art. 25 Abs. 2 DSGVO darauf ab, auch die individuellen Softwareeinstellungen so nutzerfreundlich wie nur möglich zu gestalten. Denn durch Abs. 2 werden Verantwortliche dazu verpflichtet, technische und organisatorische Maßnahmen zu ergreifen, die dafür sorgen sollen, dass bereits beim Beginn der Verarbeitung die Software so eingestellt ist, dass nur die personenbezogenen Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck zwingend notwendig sind. Dabei soll die Anzahl der erhobenen Daten, der Umfang der Verarbeitung und die Speicherdauer sowie die Zugänglichkeit zu den

584 *Hartung* (2020), Art. 25 Rn. 15; *Nolte/Werkmeister* (2018), Art. 25 Rn. 16 f.
585 *Martini* (2021), Art. 25 Rn. 29; *Hartung* (2020), Art. 25 Rn. 16; *Nolte/Werkmeister* (2018), Art. 25 Rn. 16 f., *EDPB,* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020 (Version 2.0), S. 25.
586 *Martini* (2021), Art. 25 Rn. 29; *Hartung* (2020), Art. 25 Rn. 16.
587 Wie in ErwG 78 S. 3 vorgeschlagen
588 *Nolte/Werkmeister* (2018), Art. 25 Rn. 16.
589 *Martini* (2021), Art. 25 Rn. 30 f.; *EDPB,* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020 (Version 2.0), S. 25.
590 *Danezis et al.,* Privacy and Data Protection by Design – from policy to engineering, 2014, S. 23 f.

Daten Berücksichtigung finden. In Art. 25 Abs. 2 S. 3 DSGVO wird der Zugang zu den Daten nochmals explizit aufgegriffen, indem betont wird, dass personenbezogene Daten nur nach Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden dürfen. Mit Art. 25 Abs. 2 DSGVO wird die Zweckbindung,[591] Datenminimierung[592] und Speicherbegrenzung[593] aus Art. 5 Abs. 1 DSGVO als zentrale Notwendigkeit bei der Konfiguration von Datenverarbeitungssystemen aufgegriffen. Der Verantwortliche wird also dazu verpflichtet, sicherzustellen, dass bereits bei der ersten Interaktion mit seinem System die Einstellungen so ausgestaltet sind, dass die datenschutzfreundlichste Nutzung für den Betroffenen möglich ist.[594] Nutzer sollten nicht erst Einstellungen anpassen müssen, um das beste Datenschutzniveau zu erreichen.[595] Ebenso sollen Betroffene bei Datenverarbeitungsvorgängen, auf die sie keinen unmittelbaren Einfluss nehmen können (bspw. die Verarbeitung von Personaldaten mit HR-Software oder die Verarbeitung von Finanzdaten durch Scoring-Unternehmen), vor datenschutzunfreundlichen Praktiken geschützt werden.[596]

Offensichtliches Ziel dieser Pflicht ist der Verbraucherschutz. Es soll verhindert werden, dass das mangelnde Wissen über Datenverarbeitungsvorgänge auf Seiten der Nutzer ausgenutzt wird.[597] Im Umkehrschluss bedeutet dies, dass eine Konfiguration des Systems hin zu weniger Datenschutz nur von der betroffenen Person ausgehen kann, wenn diese sich bewusst dafür entscheidet.[598] Ebenso wird teilweise davon ausgegangen, dass die Verpflichtung zu datenschutzfreundlichen Voreinstellungen und deren Fokus auf Zweckbindung und Datenminimierung, der Eindämmung von überbordenden Big-Data-Sammlungen dienlich sein soll.[599]

---

591 *Baumgartner* (2018), Art. 25 Rn. 18.

592 *EDPB,* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020 (Version 2.0), S. 12 ff.

593 *Hansen* (2019), Art. 25 Rn. 40.

594 *Hartung* (2020), Art. 25 Rn. 24.

595 *Baumgartner* (2018), Art. 25 Rn. 17.

596 *Hansen* (2019), Art. 25 Rn. 43.

597 *Baumgartner/Gausling,* ZD 2017, S. 308 (312); *Martini* (2021), Art. 25 Rn. 13 u. 46; *Wolff* (2017), Rn. 838.

598 *Baumgartner* (2018), Art. 25 Rn. 17; in Bezug auf das Setzten von Cookies*: Datenschutzkonferenz,* Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 9 ff.; in Bezug auf Dark Patterns: *Martini* (2021), Art. 25 Rn. 46a.

599 *EDPB,* Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020 (Version 2.0), S. 12 ff.; *Martini* (2021), Art. 25 Rn. 44 f.; *Nolte/Werkmeister* (2018), Art. 25 Rn. 28.

2. Beispiele für datenschutzfreundliche Voreinstellungen

Bereits 2019 entschied der EuGH, dass eine vorausgefüllte Checkbox beim Setzen von Cookies keine rechtswirksame Einwilligung darstellt.[600] Analog lässt sich dies auf Art. 25 Abs. 2 DSGVO übertragen, womit die Pflicht der datenschutzfreundlichen Voreinstellung bei Cookies nur dann erfüllt ist, wenn diese nicht standardmäßig gesetzt werden.[601]

Bei Social-Media-Diensten gilt bspw., dass der Zugriff auf Adressbücher, Standortdaten, anderweitig abgespeicherte Medien und weitere Gerätefunktionen nur dann möglich sein sollte, wenn die betroffene Person dem ausdrücklich zustimmt.[602] Auch gilt für Anbieter von Online-Diensten, wie z.B. Online-Spielen, dass diese hinterlegte Kontaktdaten nicht standardmäßig mit anderen Nutzern/Spielern des Dienstes teilen.[603]

V. Adressat der Reglungen

1. Nur Verantwortliche verpflichtet

Die Verpflichtungen aus Art. 32 und Art. 25 DSGVO richten sich unmittelbar an den Verantwortlichen der Datenverarbeitung. Gemäß Art. 4 Nr. 7 DSGVO sind Verantwortliche alle natürlichen oder juristischen Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Somit wird bewusst nicht unter verschiedenen Verantwortlichen anhand von Größe, Branche o.ä. unterschieden.[604] Nicht von den Vorgaben betroffen sind Hersteller oder Anbieter von datenverarbeitenden Produkten oder Diensten, was gemeinhin kritisch gesehen wird.[605] In ErwG. 78 S. 4 findet sich allerdings eine Ermutigung ggü. den Herstellern von Anwendungen, sich ebenso an die Vorgaben aus Art. 25 DSGVO zu halten, um sicherzustellen, dass Verantwortliche ihren Pflichten

600 EuGH, Urt. v. 1.10.2019 – (Planet49), ZD 2019, 556.
601 *Datenschutzkonferenz,* Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 13; *Martini* (2021), Art. 25 Rn. 47b.
602 *Hartung* (2020), Art. 25 Rn. 24; *Wolff* (2017), Rn. 838.
603 *Nolte/Werkmeister* (2018), Art. 25 Rn. 27.
604 *Lang* (2019)*, 4. Aufl.,* Art. 25 Rn. 26.
605 *Lang* (2019)*, 4. Aufl.,* Art. 25 Rn. 27 f.; *Martini* (2021), Art. 25 Rn. 25; *Mantz* (2018), Art. 25 Rn. 17; *Hansen* (2019), Art. 25 Rn. 21.

auch nachkommen können. Demnach wird oftmals von einer mittelbaren Wirkung ggü. Herstellern und Anbietern von datenverarbeitenden Anwendungen ausgegangen, da diese, um weiterhin am Markt bleiben zu können, zwangsläufig datenschutzfreundliche Anwendungen entwickeln müssten.[606] Ebenso würde eine Verpflichtung der Hersteller auch zur Einschränkung deren wirtschaftliche Freiheit führen, welche durch Art. 12 und 14 GG geschützt wird.[607] Dem kann wiederum entgegengehalten werden, dass ein vergleichbarer Eingriff in die wirtschaftliche Freiheit auch auf Seiten des Verantwortlichen vorliegt, der aber sehr wohl durch Art. 25 Abs. 1 DSGVO verpflichtet wird.

2. Probleme mit der alleinigen Verpflichtung von Verantwortlichen

Es ist allerdings fraglich, ob eine mittelbare Anwendung der Reglung auf Hersteller tatsächlich Wirkung entfalten kann. In der Softwareentwicklung scheint Datenschutz bzw. der Teilaspekt Sicherheit von Software häufig aus Zeitgründen vernachlässigt zu werden. Bei einer Umfrage aus 2020 gaben 79 % der Befragten an, dass sie regelmäßig bis gelegentlich unsicheren Softwarecode veröffentlichen würden.[608] In 54 % der Fälle geschieht dies, um kritische Deadlines einzuhalten.[609] Diese Priorisierung von der Bereitstellung der Funktionalität bzw. Einhaltung von Deadlines über Sicherheit und Datenschutz könnte zwei wesentliche Gründe haben. Erstens scheint auf Seiten von Softwareentwicklern häufig noch eine Unwissenheit bzgl. Datenschutz durch Technikgestaltung zu bestehen und oftmals stehen auch keine entsprechenden Ressourcen (Tools, Unterstützung etc.) zur Verfügung, die die Umsetzung erleichtern würden.[610] Zweitens scheint es auch nur wenige Forschungsergebnisse zur praktischen Umsetzung von Art. 25 DSGVO in der Softwareentwicklung zu geben.[611] Demnach kann nur auf wenige Erkenntnisse aus der empirischen Wissenschaft zurückgegriffen werden. Diese beiden Punkte sind nicht verwunderlich, wenn man

606 *Baumgartner/Gausling,* ZD 2017, S. 308 (311); *Schulz,* CR 2012, S. 204 (207); *Hartung* (2020), Art. 25 Rn. 13.
607 *Schulz,* CR 2012, S. 204 (207); *Hartung* (2020), Art. 25 Rn. 13.
608 Abrufbar unter: https://www.veracode.com/sites/default/files/pdf/resources/survey reports/esg-modern-application-development-security-veracode-survey-report.pdf (abgerufen 15.5.2022).
609 Ebenda.
610 *Alhazmi/Arachchilage,* Personal and Ubiquitous Computing 2021, S. 879 (885 ff.).
611 *Morales-Trujillo et al.,* CLEI Electronic Journal 2019, S. 1 (20 ff.).

bedenkt, dass aus Art. 25 DSGVO keine direkte Notwendigkeit für Softwareentwickler (solange diese nicht gleichzeitig auch Verantwortliche sind) hervorgeht, diese Datenschutzprinzipien zu praktizieren.

Dieser Umstand macht es auch für Verantwortliche komplizierter, ihren Pflichten nachzukommen. Denn wenn am Markt, u.a. wegen der soeben dargelegten fehlenden Anreize für Softwareentwickler, keine datenschutzfreundliche Version einer notwendigen Anwendung existiert, können Verantwortliche nur auf vorhandene, weniger datensparsame Technologien zurückgreifen.[612] Besonders bei Angeboten von Unternehmen mit ausgeprägter Marktdominanz, wie z.B. Google,[613] Facebook[614] oder Microsoft,[615] bestehen für Verantwortliche Lock-In Effekte. Deutlich wird dies bei den Web-Analyse-Tools von Google. Diese Tools können kombiniert einen weltweiten Marktanteil von mehr als 70 % aufweisen.[616] Zwar gibt es bereits einige datenschutzfreundlichere Alternativen, jedoch sind diese meist unbekannt und scheinen kein vollwertiger Ersatz zum kostenfreien Google Angebot zu sein. Ein Wechsel käme für viele Verantwortliche damit wahrscheinlich nicht in Frage. Trotz der erheblichen Datenschutzdefizite der Tools, ist davon auszugehen, dass die Verpflichtung des Verantwortlichen gemäß Art. 25 DSGVO nicht zu einem Abwenden von Google führen wird. Dies könnte auch ein Grund dafür sein, warum einige europäische Länder nun ein Verbot dieser Software in Erwägung ziehen.[617]

Hinzu kommt, dass bei einer alleinigen Verpflichtung der Verantwortlichen in Kombination mit ausgeprägter Marktdominanz einiger Anbieter und den damit einhergehenden Lock-In Effekten, Anwendungen wie z.B. die Web-Analyse-Tools von Google letztendlich den Stand der Technik

612 *Martini* (2021), Art. 25 Rn. 25.

613 Abrufbar unter: https://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/ (abgerufen 15.5.2022).

614 Abrufbar unter: https://de.statista.com/statistik/daten/studie/241601/umfrage/marktanteile-fuehrender-social-media-seiten-weltweit/ (abgerufen 15.5.2022).

615 Abrufbar unter: https://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/ (abgerufen 15.5.2022).

616 Aufrufbar unter: https://www.statista.com/statistics/1258557/web-analytics-market-share-technology-worldwide/ (abgerufen 15.5.2022).

617 Österreich: Abrufbar unter: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf (abgerufen 15.5.2022); Niederlande: Abrufbar unter: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#hoe-kan-ik-bij-google-analytics-de-privacy-van-mijn-websitebezoekers-beschermen-4898 (abgerufen 15.5.2022); Luxemburg: Abrufbar unter: https://www.datenschutzstelle.li/aktuelles/google-analytics-und-der-datenschutz (abgerufen 15.5.2022).

abbilden, womit ebenso eine Weiterentwicklung hin zu datenschutzfreundlichen Alternativen verhindert werden könnte.[618]

VI. Technischer Datenschutz bei BCI

Um eine sichere Verarbeitung von Wesensdaten zu gewährleisten, bedarf es einer ausreichenden Gewährleistung der Datensicherheit. Nachfolgend sollen darum einige Maßnahmen vorgestellt werden, die dafür geeignet sind. Die Auswahl soll lediglich die sinnvollsten Gestaltungsmöglichkeiten aufzeigen und ist somit nicht abschließend.

1. Bewertung von BCI

In Art. 32 Abs. 1 sowie Art. 25 Abs. 1 DSGVO macht der Gesetzgeber deutlich, dass bei der Auswahl von geeigneten Maßnahmen Art, Umfang, Umstände, Zwecke der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere der Risiken sowie Stand der Technik und Implementierungskosten berücksichtigt werden sollen. Um entsprechende Maßnahmen für BCI zu definieren, bedarf es demnach einer vorherigen Auseinandersetzung mit diesen Vorgaben.

a. Art, Umfang, Umstände und Zwecke der Verarbeitung

Durch BCI können Wesensdaten in verschiedensten Arten verarbeitet werden. Wahrscheinlich ist eine Erhebung, Erfassung, Speicherung, Auswertung und auch Übermittlung. Besonders ist dabei, dass mit Wesensdaten Daten vorliegen, die ein noch nie zuvor dagewesenes Auswertungspotential besitzen, auch wenn diese rechtlich nicht zwangsläufig als besondere Kategorien von personenbezogenen Daten einzustufen sind.

Da durch BCI in vielen Fällen die Gehirnaktivitäten ständig ausgelesen, erhoben und ausgewertet werden müssen, ist die damit einhergehende Verarbeitung auch als entsprechend umfangreich einzustufen. Besonders wenn man davon ausgeht, dass der Verantwortliche die Daten von etlichen BCI-Nutzern verarbeitet.

618 *Hartung* (2020), Art. 25 Rn. 13.

Die Datenverarbeitung folgt dabei für gewöhnlich vier Schritten: 1. Signalaufzeichnung, 2. Extraktion von relevanten Signalen, 3. Übersetzung der relevanten Signale und 4. Output-Generierung.[619] Zu Beginn werden bei der Signalaufzeichnung die Gehirnaktivitäten mithilfe von Sensoren aufgezeichnet. Dafür können verschiedene Technologien eingesetzt werden, die in Kapitel C.I.I.a und b. genauer thematisiert werden. Da bei der initialen Aufzeichnung der Gehirnaktivitäten auch weitere, irrelevante Stör- und Hintergrundsignale aufgezeichnet werden, müssen fortführend die für die Handlung relevanten Signale isoliert und extrahiert werden.[620] Dies wird automatisiert durch eine Signalverarbeitungs-Software vorgenommen.[621] Erst danach kann mithilfe eines Übersetzungsalgorithmus eine Konvertierung der relevanten Signale zu entsprechenden Befehlen stattfinden.[622] Dieser Befehl wird abschließend an das externe Gerät weitergeleitet, welches dann den gewünschte Output erzeugt.[623] Um die Zusammenarbeit dieser einzelnen Schritte und die Interaktion mit dem Nutzer zu überwachen, bedarf es übergeordnet noch einer einheitlichen Betriebsumgebung, bei der alle Funktionen zusammenlaufen, koordiniert und kontrolliert werden.[624] Mit BCI wird somit eine hochtechnisierte Verarbeitung von Wesensdaten ermöglicht. Die Dauer dieser Verarbeitung ist damit erstmal nicht begrenzt, sondern findet so lange statt, wie eine Person ein BCI nutzt. Dementsprechend ist davon auszugehen, dass die entsprechenden Wesensdaten auch mindestens so lange gespeichert werden. Es ist ebenso denkbar, dass die Daten in Zukunft über die Nutzungsdauer hinweg gespeichert werden könnten, um die Algorithmen und das eingesetzte System als solches zu verbessern.

Der Zweck der Verarbeitung von Wesensdaten von BCI kann sich vielfältig gestalten. Vereinfacht formuliert möchten Verantwortliche mit der Datenverarbeitung ermöglichen, dass mithilfe von Gehirnsignalen gewünschte Outputs erzeugt werden können. Unabhängig davon, welche Outputs ge-

619 *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (270).
620 *Krusienski/McFarland/Principe,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 123 (123).
621 *Guger et al.*, in: Guger et al., Brain-Computer Interface Research, 2019, S. 1 (1); *Wilson/Guger/Schalk,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 165 (176 ff.).
622 *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (272); detaillierter: *McFarland/Krusienski,* in: Wolpaw/Winter Wolpaw, Brain-Computer Interfaces, 2012, S. 147 (147 ff.).
623 *Shih et al.,* Mayo Clinic Proceedings 2012, S. 268 (272).
624 *Guger et al.*, in: Guger et al., Brain-Computer Interface Research, 2019, S. 1 (1).

nau gewünscht sind, handelt es sich dabei prinzipiell um einen sehr invasiven und weitreichenden Verarbeitungszweck, da zu jeder Zeit Wesensdaten verarbeitet werden.

b. Eintrittswahrscheinlichkeit und Schwere der Risiken

Wie in Kapitel I.I.1 bereits dargelegt wurde, steigt die Bedrohung durch Cyberangriffe weltweit. Meist werden mit solchen Attacken finanzielle Interessen verfolgt.[625] Dabei wird häufig von Erpressung Gebrauch gemacht, indem bspw. gedroht wird, dass bei Nichtzahlung einer geforderten Geldsumme eine Veröffentlichung von sensiblen Daten stattfindet.[626] Daneben werden gestohlene Daten aber auch klassisch im Internet zum Kauf angeboten.[627] Die Käufer der Daten können diese dann wiederum z.B. für Identitätsdiebstahl, Betrug oder Erpressung nutzen.

Wesensdaten zeichnen sich durch ihr unvergleichbares Informationsschöpfungspotential aus. Sie können Aussagen über die politische Meinung machen,[628] teilweise die religiöse oder weltanschauliche Überzeugung offenbaren,[629] die sexuelle Orientierung und das Sexualleben offenlegen,[630] als Gesundheitsdaten definiert werden,[631] als biometrische Daten die eindeutige Identifizierung einer natürlichen Person ermöglichen[632] und noch vieles mehr (s. Kapitel B.III.1-2 u. D.I.). Dementsprechend werden diese

625 Abrufbar unter: https://www.verizon.com/business/resources/reports/dbir/2020/results-and-analysis/ (abgerufen 4.12.2022).

626 *Bundesamt für Sicherheit in der Informationstechnik,* Die Lage der IT-Sicherheit in Deutschland 2022, v. 25.10.2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410, S. 13 ff., 52 (abgerufen 4.12.2022).

627 Übersicht von gängigen Preisen für verschiedene Datensätze: *Ruffio,* Dark Web Price Index 2022, v. 19.9.2022, https://www.privacyaffairs.com/dark-web-price-index-2022/ (abgerufen 4.12.2022).

628 *Schreiber et al.,* PLOS ONE 2013, S. 1 (2f.); *Vecchiato et al.,* 31st Annual International Conference of the IEEE EMBS 2009, S. 57 (59f.).

629 *Knutson et al.,* Human Brain Mapping 2007, S. 915 (927).

630 *Safron et al.,* Scientific Reports 2018 (8), S. 1 (7 ff.); *Hammilton/Meston,* Archive of Sexual Behavior 2017, S. 2289 (2294 f.).

631 *Bansal/Mahajan,* EEG-Based Brain-Computer Interfaces: Cognitive Analysis and Control Applications, 2019, S. 61; *Mattia/Molinari,* in: Grübler/Hildt, Brain-Computer Interfaces in their ethical, social and cultural contexts, 2014, S. 49 (50f); *Sebastián-Romagosa et al.,* Frontiers of Neuroscience 2020, S. 1 (5).

632 *Landau/Puzis/Nissim,* AMC Computing Surveys 2020, S. 1 (12 ff.); *Qui et al.,* ACM Computing Surveys 2019, S. 1 (3 ff.).

Daten in Zukunft auch besonders interessant für böswillige Erpressungs- und Betrugsversuche sein. Sollten bspw. Wesensdaten vorliegen, aus denen hervorgeht, dass eine stigmatisierte psychische Erkrankung vorliegt oder die betroffene Person unliebsame politische Meinungen hat, können diese von unbefugten Dritten dafür genutzt werden, um den entsprechenden Nutzer zu erpressen. Auch Identitätsdiebstahl wäre möglich, wenn in Zukunft bspw. Gehirnsignale zur Authentifizierung eingesetzt werden und dann in böswillige Hände gelangen.

Sobald die Verbreitung von BCI steigt, ist demnach mit einer hohen Eintrittswahrscheinlichkeit und Schwere der Risiken für Betroffene zu rechnen.

c. Stand der Technik und Implementierungskosten

In der Praxis haben sich bereits einige Verfahren und Maßnahmen durchgesetzt und bewährt, um die IT-Sicherheit zu steigern. Auf dieses Wissen kann die Sicherheitsinfrastruktur von BCI aufbauen. Wie fortfolgend gezeigt wird, können gängige Mittel das Sicherheitsniveau bereits deutlich steigern. Daneben können weitere bereits bei anderen Technologien eingesetzte Verfahren auf BCI übertragen werden, um die Sicherheit zu erhöhen. Damit können die Implementierungskosten auch gering gehalten werden, da keine eigene Forschung und Entwicklung mehr notwendig ist und auf etablierte Software-Angebote zurückgegriffen werden kann. Der Stand der Technik reicht demnach zunächst aus, um eine dem Risiko angemessene Datensicherheit zu vertretbaren Implementierungskosten zu gewährleisten.

2. Datenschutz durch Technikgestaltung und technische und organisatorische Maßnahmen bei BCI

Anhand der vorausgegangenen Auseinandersetzung mit den relevanten Auswahlkriterien können diverse Maßnahmen empfohlen werden, um die Sicherheit der Datenverarbeitung zu steigern.

a. Pseudonymisierung von Wesensdaten

Als explizites Beispiel einer sinnvollen Maßnahme nennt Art. 25 Abs. 1 DSGVO die Pseudonymisierung von personenbezogenen Daten. Wie bereits dargelegt, werden personenbezogene Daten mithilfe dieser Maßnahme in einer Art und Weise verarbeitet, bei der es ohne Hinzuziehung von weiteren Informationen nicht mehr möglich ist, diese einer spezifischen betroffenen Person zuzuordnen. Dies wird dadurch gewährleistet, dass vorliegende Identifikationsmerkmale, wie z.B. ein Name, durch anderweitige Ziffern oder Kennzeichen ersetzt werden, welche nur mit einer entsprechenden Regel oder Zusatzinformation erneut der betroffenen Person zugeordnet werden können.[633] Dieses Vorgehen könnte auch bei BCI Anwendung finden. So könnten ausgelesene Gehirnaktivitäten bspw. mit entsprechenden pseudonymisierten Kennnummern verknüpft werden. Bei einer ungewollten Datenoffenlegung hätte dies zum Vorteil, dass eine Zuordnung der abgeflossenen Daten zu einer bestimmten Person nicht direkt und nur mit ergänzendem Aufwand möglich wäre.

b. Anonymisierung von Wesensdaten

Weiter als die Pseudonymisierung geht die Anonymisierung. Dabei wird jeglicher Personenbezug von Daten entfernt, sodass keine Zuordnung zu einer natürlichen Person mehr möglich ist, auch mit Zusatzinformationen nicht. Bei einer vollständigen Anonymisierung lägen somit keine personenbezogenen Daten mehr vor und die DSGVO würde gemäß ErwG. 26 auch keine Anwendung mehr finden.[634] Wie etliche Untersuchungen zeigen, ist die Erreichung einer vollständigen Anonymisierung allerdings eine große Herausforderung. Eine Studie zu Forschungsdaten schaffte es bspw., 96 % der betrachteten anonymisierten Datensätze mithilfe von Diagnosen/Diagnosecodes erneut den (dann erneut identifizierten) Personen zuzuordnen.[635] Eine weitere Untersuchung nutzte Gesichtsmodellierungs- und Erkennungs-Software, um Personen mithilfe von anonymisierten MRT-Scans ihrer Köpfe zu identifizieren.[636] Sich dem anschließend, kommt eine Studie

633 *Jandt* (2020), Art. 32 Rn. 18.
634 *Ernst* (2021), Art. 4 Rn. 48.
635 *Loukides/Denny/Malin,* Journal of the American Medical Informatics Association 2010, S. 322 (323 ff.).
636 *Schwarz et al.,* The New England Journal of Medicine 2019, S. 1684 (1684 ff.).

zum Schluss, dass 99,98 % der anonymisierten Personen mithilfe von 15 demografischen Attributen re-identifiziert werden könnten, was die Autoren zu der Einschätzung veranlasst, dass auch sorgfältig anonymisierte Datensätze meist nicht den Anforderungen der DSGVO gerecht werden dürften.[637]

In Bezug auf BCI wäre die Umsetzung einer vollständigen Anonymisierung wünschenswert. Damit würden zumindest die möglichen individuellen Folgen für Betroffene nach Datenoffenlegung o.Ä. beseitigt werden. Wie die allgemeine Forschung zu Anonymisierung allerdings zeigt, ist dies oftmals kaum möglich. Hinzu kommt, dass gewisse Gehirndaten einzigartig sind und darum bspw. auch als Authentifizierungs- bzw. Identifizierungsmaßnahmen Verwendung finden.[638] Demnach stellt sich ganz grundlegend die Frage, ob neurologische Daten überhaupt anonymisiert werden können. Zwar gab es schon Bestrebungen, eine vollständige Anonymisierung von Gehirndaten zu erreichen, bislang blieb dies aber ohne Erfolg.[639] Nichtsdestotrotz ist dies ein Ansatz, der bei BCI weiterverfolgt werden sollte.

c. Verschlüsselung

Sobald personenbezogene Daten technisch übermittelt werden, ist eine Verschlüsselung zu empfehlen. Aus diesem Grund nennt Art. 32 Abs. 1 lit. a DSGVO diese Maßnahme auch explizit als Beispiel, um die Sicherheit der Verarbeitung zu erhöhen. Verschlüsselung bedeutet, dass die klare Lesbarkeit von Daten mithilfe von kryptografischen Mitteln so angepasst wird, dass die Daten nur noch mit dem richtigen Schlüssel ausgelesen werden können.[640] Damit soll sichergestellt werden, dass unbefugte Personen keinen Zugang zu personenbezogenen Daten erhalten.[641] Dies kann sowohl durch symmetrische (Kommunikationspartner besitzen denselben geheimen Schlüssel zum Ver- und Entschlüsseln)[642] als auch asymmetrische

637 *Rocher/Hendrickx/de Montojoye,* Nature Communications 2019, S. 1 (1 ff.).
638 *Landau/Puzis/Nissim,* AMC Computing Surveys 2020, S. 1 (12 ff.).
639 Wie ein aufgegebenes Patent zeigt: Abrufbar unter: https://patents.google.com/patent/US20140228701A1/en (abgerufen 23.10.2022).
640 *Mantz* (2018), Art. 32 Rn. 11.
641 *Piltz* (2018), Art. 32 Rn. 28.
642 *Petrlic/Sorge,* Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, 2017, S. 15.

(Kommunikationspartner besitzen unterschiedliche Schlüssel zum Ver- und Entschlüsseln)[643] Verschlüsslungsverfahren gelingen.[644]

Da bei BCI ständig eine Übermittlung von hoch sensitiven personenbezogenen Daten stattfindet, wird eine Implementierung einer aktuellen und sicheren Verschlüsselung empfohlen.[645] Dabei sollte aktuellen Forschungsansätzen gefolgt werden, bei denen Gehirnsignale mithilfe von kryptographischen Mitteln nur den betroffenen Personen offengelegt werden und sonst niemand anderem, ohne die Funktion des Gerätes zu behindern.[646] Bei der Auswahl der kryptographischen Mittel sollten auch biometrische Verschlüsselungstechnologien in Betracht gezogen werden, die direkt auf den einzigartigen Gehirnsignalen der Nutzer aufbauen.[647] Dafür wird bspw. mithilfe eines kurzen EEG-Scans ein randomisierter Schlüssel erstellt, um nachfolgend die gewünschten Daten zu verschlüsseln. Zum Entschlüsseln braucht es einen weiteren EEG-Scan, der dann einen ergänzenden Schlüssel erzeugt, um die Daten wieder zu entschlüsseln.[648]

d. Angriffsschutz

Für Unternehmensanlagen oder Serverfarmen gehören Firewalls bereits zur Grundausstattung. Auch für allgemeine, medizinische Hilfsgeräte ist eine solche, auf die besonderen Gegebenheiten abgestimmte Firewall, bereits programmiert worden.[649] Die Software überwacht dabei jegliche Kommunikation von/mit dem Gerät, um mithilfe von Algorithmen Anomalien in den Transaktionen zu erkennen. Sobald verdächtige Kommunikation entdeckt wird, werden Sicherheitsmaßnahmen ergriffen, die von einer ein-

643 Ebenda, S. 16.
644 *Jandt* (2020), Art. 32 Rn. 19.
645 Bzgl. (medizinische) Implantate: *Droste et al.,* Current Directions in Biomedical Engineering 2018, S. 1 (16); *Browning/Tuma,* South Carolina Law Review 2016, S. 637 (653).
646 *Agarwal et al.,* IEEE Transactions on Neural Systems and Rehabilitation Engineering 2019, S. 1546 (1549 ff.).
647 *Ravi et al.,* IEEE Conference on Computational Intelligence and Multimedia Applications 2007, S. 1 (1 ff.); *Rajendra/Rajeneesh,* International Journal of Scientific and Engineering Research 2011, S. 1 (1 ff.); *Bajwa/Dantu,* Computers & Security 2016, S. 95 (95 ff.).
648 *Ravi et al.,* IEEE Conference on Computational Intelligence and Multimedia Applications 2007, S. 1 (1 ff.).
649 *Zhang/Raghunathan/Jha,* IEEE Transactions on Biomedical Circuits and Systems 2013, S. 871 (871 ff.).

fachen Benachrichtigung des Nutzers, bis hin zum Abriegeln des Systems reichen können.[650] Diese dabei gesammelten Erkenntnisse und Erfahrungen könnten auf BCI angewendet werden, indem eine entsprechende Software für den Schutz von Gehirnsignalen entwickelt wird.[651] Je nach System könnte dafür bspw. ein Schwellenwert an Kommunikations-Intervallen und -Frequenzen festgelegt werden, sodass Überschreitungen dieser Werte als mögliche Anomalien auftauchen.[652] Ebenso könnte eine Identifikation von verdächtigten Befehlen stattfinden, sodass bspw. offensichtlich gegensätzliche oder für den Nutzer unübliche Befehle als auffällig gelten.[653] Auch könnten bestimmte Befehle, die grundsätzlich ein hohes Risiko für Benutzer mit sich bringen, nur nach ausdrücklicher Freigabe der Nutzer möglich sein (z.B. biometrische Freischaltung).

Neben der Implementation einer BCI-spezifischen Firewall wäre das Führen einer Log-Datei ebenso empfehlenswert. In dieser könnten alle Aktivitäten, die das BCI betreffen, protokolliert und regelmäßig auf Anomalien überprüft werden.[654] Eine weitere Maßnahme, um insbesondere DoS-Attacken vorzubeugen, wäre das Priorisieren von Anfragen, indem bspw. Kernfunktionen jederzeit Vorzug erhalten.[655] Abschließend sind ebenso Anti-Viren-Anwendungen für BCI empfehlenswert.[656]

e. Sichere Authentifizierung

Eine weitere, simple Maßnahme, um unbefugten Zugang zu verhindern, ist eine Benutzer-Authentifizierung.[657] Dabei ist auch eine Berechtigungsverwaltung denkbar, bei der Befugnisse erst freigeschaltet werden müssen.[658] Grundsätzlich sollten BCI dabei mittels Zwei-Faktor-Authentifizierung ge-

650 *Ebenda.*
651 *Takabi,* IEEE Conference on Communications and Network Security 2016, S. 1 (1 f.).
652 *Landau/Puzis/Nissim,* AMC Computing Surveys 2020, S. 1 (30); *Takabi,* IEEE Conference on Communications and Network Security 2016, S. 1 (1 f.); Bzgl. medizinische Implantate: *Konstadinov,* Hacking Implantable Medical Devices, v. 28.4.2014, https://resources.infosecinstitute.com/topic/hcking-implantable-medical-devices/ (abgerufen 12.11.2022).
653 *Ebenda.*
654 *Hassija et al.,* Sustainable Cities and Society 2020, S. 1 (7).
655 *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (212 f.).
656 *Bernal et al.,* ACM Computing Surveys 2022, S. 1 (14).
657 *Martini* (2021), Art. 32 Rn. 35d.
658 *Hassija et al.,* Sustainable Cities and Society 2020, S. 1 (7).

schützt werden, sodass die Kenntnis über Nutzername und Kennwort nicht schon ausreicht, um Zugang zu einem Gerät zu erhalten.[659] Dies ist besonders geboten, da die meisten selbstgewählten Passwörter bzw. der Umgang mit diesen im privaten Bereich oftmals nicht sicher sind. So nutzen bspw. viele Menschen dasselbe Passwort für verschiedene Dienste[660] und ca. 27 % schreiben ihre Passwörter auf Zettel und legen diese dann ab.[661]

f. Unterbindung von ständiger Aufzeichnung

Um eine ständige anlasslose Aufzeichnung von Wesensdaten bei BCI-Nutzern zu verhindern, könnte ein ähnlicher Ansatz wie bei Smart Speakern Anwendung finden. Bei Smart Speakern handelt es sich um Lautsprecher, die mit dem Menschen interagieren können, indem sie durch gezielte Sprachbefehle aktiviert werden und bestimmte Aufgaben erledigen können. Smart Speaker sind BCI demnach sehr ähnlich, nur weniger invasiv, was die Datenverarbeitung betrifft.

Bei Smart Speakern hat sich die Funktionsweise durchgesetzt, bei der zuerst eine Aktivierung durch ein bestimmtes Keyword (z.B. „Alexa", „Okay Google") stattfinden muss, damit eine Spracheingabe getätigt werden kann, worauf eine Spracherkennung folgt, die wiederum für die Umsetzung der identifizierten Anfrage relevant ist, sodass mit der finalen Sprachausgabe die gewünschte Antwort oder Auskunft gegeben werden kann.[662] Um diesen Ablauf zu gewährleisten, muss die zugrundeliegende Software passiv dauernd mithören, um bei der Artikulation des Keywords umgehend aktiviert werden zu können.[663] Erst nach einer Aktivierung wird die darauffolgende Sprachsequenz tatsächlich aufgezeichnet und verarbeitet.[664]

---

659 Anderer Meinung: *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (212) – gehen davon aus, dass nur bei invasiven BCI 2FA notwendig ist.

660 Abrufbar unter: https://de.statista.com/statistik/daten/studie/1092721/umfrage/passworterstellung-fuer-online-dienste-in-deutschland/ (abgerufen 12.11.2022); Abrufbar unter: https://de.statista.com/statistik/daten/studie/818713/umfrage/nutzung-von-unterschiedlichen-passwoertern-fuer-unterschiedliche-dienste-in-deutschland/ (abgerufen 4.1.2025).

661 Abrufbar unter: https://de.statista.com/statistik/daten/studie/818850/umfrage/ablage-von-passwoertern-in-deutschland/ (abgerufen 12.11.2022).

662 *Anke/Fischer/Lemke,* in: Räckers et al., Digitalisierung von Staat und Verwaltung, 2019, S. 25 (27).

663 *Hoy,* Medical Reference Services Quarterly 2018, S. 81 (82).

664 *Anke/Fischer/Lemke,* in: Räckers et al., Digitalisierung von Staat und Verwaltung, 2019, S. 25 (27).

Ein solcher Ansatz wäre analog auch bei BCI möglich. Dies wäre umsetzbar, indem Nutzer einen physischen Knopf am Gerät betätigen oder ein bestimmtes Gehirnsignal festlegen müssen, welches zur Aktivierung der Software dient. Erst nach dieser Aktivierung wird dann eine Datenverarbeitung vorgenommen. Die Verarbeitung kann durch den Nutzer ebenso auf demselben Weg wieder unterbunden werden. Ergänzend dazu sollte die Software so eingestellt sein, dass sich diese bei einer gewissen Zeit an Inaktivität (Zeit, in der kein neurologisches Signal in einen Output umgewandelt wird) automatisch selbst ausschaltet. Dieses Vorgehen würde dem Prinzip der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO gerecht werden und der Privatsphäre der BCI-Nutzer dienlich sein, da nicht alle ihre Gehirnaktivitäten ständig aufgezeichnet werden würden, sondern nur jene, die erwünscht und notwendig sind.

g. Datenminimierung

Ergänzend zur Unterbindung einer ständigen Aufzeichnung, sollte auch gelten, dass nur die Daten verarbeitet werden, die für die spezifische Funktion tatsächlich notwendig sind. Dazu sollten BCI besser dynamisch gestaltet sein, sodass automatisiert oder benutzergesteuert nur solche Elektroden aktiviert sind, die benötigt werden.[665] Damit minimiert man den Umfang der erhoben Wesensdaten erheblich. Ergänzend könnten BCI erhobene Daten auch noch automatisiert vorfiltern, sodass bspw. mögliche Dritte gar nicht erst unnötige Rohdaten oder Daten, die nicht für die Funktion notwendig sind, erhalten.[666]

h. Organisatorische Maßnahmen

Neben den technischen Maßnahmen sollten Verantwortliche bei der Verarbeitung von Wesensdaten auch organisatorische Maßnahmen nicht außer Acht lassen. Besonders erwähnenswert ist hierbei die initiale und kontinuierliche Schulung von Mitarbeitern. Damit kann sichergestellt werden, dass alle Personen über relevante IT-Sicherheits- und Datenschutz-Themen informiert bleiben, entsprechend weniger anfällig für bspw. Phishing, Social-Engineering o.Ä. sind und bedächtiger mit Daten umgehen. Dieses

665 *Bernal et al.,* ACM Computing Surveys 2022, S. 1 (13).
666 *Martini/Kemper,* International Cybersecurity Law Review 2022, S. 191 (213).

Bewusstsein kann durch verbindliche interne Richtlinien zu z.B. Umgang und Gestaltung von Passwörtern, Umgang mit Datenträgern, Vorgehen bei Sicherheitsvorfällen etc. gestärkt werden. Im Zuge dessen sollten Mitarbeiter auch Vertraulichkeitsverpflichtungen unterzeichnen, um die Relevanz von Datenschutz hervorzuheben.

Daneben sind Zugangs- und Berechtigungskonzepte maßgeblich. Der Zugang zu den Datenverarbeitungsanlagen und -systemen sollten nur den Personen ermöglicht werden, die diesen auch tatsächlich benötigen. Ergänzende Authentifizierungsmechanismen können dabei sicherstellen, dass auch nur solche Zugänge bzw. Berechtigungen gewährt werden, die für die jeweilige Aufgabenerledigung tatsächlich notwendig sind.

Abschließend sollten auch umfassende Backup- und Recovery-Konzepte vorhanden sein sowie regelmäßige, diesbezügliche Tests durchgeführt werden. Entsprechende Ergebnisse sind dann zu protokollieren. Damit garantiert man funktionierende Abläufe bei Notfällen und kann frühzeitig Anpassungsbedarfe identifizieren.

3. Datenschutzfreundliche Voreinstellungen bei BCI

Auch bei BCI sollten die Voreinstellungen so konzipiert werden, dass eine Konfiguration des Systems hin zu weniger Datenschutz nur von der betroffenen Person ausgehen kann, wenn diese sich bewusst dafür entscheidet.[667] Dies bedeutet somit, dass BCI so eingestellt werden müssen, dass mit erster Inbetriebnahme nur jene Wesensdaten verarbeitet werden, die für den Nutzungszweck tatsächlich notwendig sind.

Wird bspw. ein BCI lediglich dazu genutzt, um einen Hilfsroboter zu steuern, sollte die standardgemäße Einstellung des Geräts nicht auch noch die Auswertung von neurologischen Signalen zur Verbesserung des Systems oder die Auswertung von neurologischen Reaktionen auf TV-Werbung erlauben.

667 *Baumgartner* (2018), Art. 25 Rn. 17; in Bezug auf das Setzten von Cookies*: Datenschutzkonferenz,* Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, S. 9 ff.; in Bezug auf Dark Patterns: *Martini* (2021), Art. 25 Rn. 46a.

J. Datenschutz-Management

Vorausgehend wurde ausführlich beschrieben, welche technischen und organisatorischen Maßnahmen bei BCI eingesetzt werden könnten, um das Risiko der Verarbeitung von Wesensdaten zu minimieren. Um eine vollständige Risikominimierung zu erhalten, sieht die DSGVO allerdings ergänzend zu jenen Maßnahmen ebenso vor, dass in relevanten Fällen auch noch eigenverantwortliche und kleinteilige Risikoanalysen von Verantwortlichen vorgenommen werden müssen.[668]

Nachfolgend soll geprüft werden, ob die Verarbeitung von Wesensdaten durch BCI einer solchen Risikoanalyse bedarf. Ebenso soll skizziert werden, wie genau eine solche Analyse aussehen könnte.

I. Notwendigkeit einer Datenschutz-Folgenabschätzung

In Art. 35 Abs. 1 S. 1 DSGVO fordert der Gesetzgeber, dass bei einigen Verarbeitungsformen eine vorherige Abschätzung möglicher Folgen für den Schutz personenbezogener Daten stattfinden muss. Wann eine solche Datenschutz-Folgenabschätzung (DSFA) notwendig ist, soll sich davon ableiten, ob der Einsatz von neuartigen Technologien und die Art, der Umfang und der Zweck der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen haben könnte. Anhand dieser Kriterien ist demnach eine vorgelagerte Schwellenwertanalyse durchzuführen.

1. Hohes Risiko

Maßgeblich für die Bewertung, ob eine DSFA notwendig ist, ist das vorhandene Risiko. Lediglich wenn ein hohes Risiko vorliegt, ist eine entsprechende Analyse notwendig. Wann genau ein hohes Risiko vorliegt, wird in der DSGVO nicht weiter konkretisiert. Grundsätzlich liegt ein solches dann vor, wenn das gewöhnliche Gefahrenpotential, das üblicherweise bei einer durchschnittlichen Datenverarbeitung zu erwarten ist, überschritten

668 *Baumgartner* (2018), Art. 35 Rn. 1.

wird.[669] Als relevante Kriterien für die Feststellung, ob dieser Schwellenwert überschritten ist, wird in Art. 35 Abs. 1 DSGVO der Einsatz von neuer Technologie und die Art, der Umfang, die Umstände und der Zweck der konkreten Verarbeitung genannt. Anhand dieser Aspekte sollen im Einzelfall vorrausschauend und ganzheitlich die Eintrittswahrscheinlichkeit und Schwere des Risikos identifiziert werden, wovon sich dann das insgesamte Risiko ableiten lässt.[670] Wichtig dabei ist, dass das insgesamte Risiko nicht als sichere Folge der Verarbeitung identifiziert werden muss, um die Notwendigkeit einer DSFA auszulösen.[671] Es reicht, wenn das Risiko als voraussichtliche Folge prognostiziert wird.[672] Dabei sollten vor allem mögliche Schäden der Verarbeitung berücksichtigt werden. ErwG. 75, 83 S. 3, und 85 S. 1 stellen fest, dass mögliche Schäden entweder materieller, immaterieller oder gar physischer Natur sein könnten. Als konkrete Beispiele werden u.a. Diskriminierung, Identitätsdiebstahl, finanzieller Verlust und Rufschädigung aufgeführt. Dabei kann schon ein einziger Faktor ausreichen, um ein hohes Risiko zu begründen.[673] ErwG. 94 S. 2 macht dies deutlich, indem bereits der Umfang der Datenverarbeitung als ausreichender Faktor benannt wird, um ein hohes Risiko auszulösen.[674]

a. Neue Technologien

Was genau die DSGVO unter Art, Umfang, Umstände und Zweck der konkreten Verarbeitung versteht, wurde bereits in Kapitel I.II.2.c dargelegt und lässt sich demnach auch auf die DSFA übertragen. Noch nicht dargelegt wurde allerdings, was mit dem Einsatz von neuer Technologie gemeint ist.

Maßgeblich für die Bewertung, ob ein hohes Risiko vorliegt, ist u.a. der Einsatz von neuer Technologie. Mit „neue Technologien" könnten sprachlich solche Technologien gemeint sein, die erst vor Kurzem neu entwickelt und auf den Markt gebracht wurden, als auch jene Technologien, die bereits etabliert sind, allerdings nun das erste Mal bei dem Verantwortlichen

669 *Laue* (2019), Art. 35 DSGVO Rn. 11; *Baumgartner* (2018), Art. 35 Rn. 22.
670 *Martini* (2021), Art. 35 Rn. 17; *Baumgartner* (2018), Art. 35 Rn. 22.
671 *Baumgartner* (2018), Art. 35 Rn. 19; *Martini* (2021), Art. 35 Rn. 19.
672 *Ebenda.*
673 *Jandt* (2020), Art. 35 Rn. 7.
674 Auch die Art.-29-Gruppe sieht den Umfang der Verarbeitung als relevantes Kriterium: *Art.-29-Gruppe*, WP 248, 2017, S. 11.

eingesetzt werden sollen.[675] In ErwG. 91 wird noch ergänzt, dass bei der Bewertung auf den Stand der Technik abgestellt werden muss.[676] Doch reicht der bloße Einsatz einer solche neuen Technologie noch nicht aus, um eine DSFA notwendig zu machen. Der Einsatz muss stattdessen auch noch mit einem hohen Risiko verbunden sein. Demnach können derzeit besonders Gesichts- und Spracherkennung, Videoüberwachung, GPS-Dienste oder auch der Einsatz von Blockchain-Technologie gewöhnlicherweise als „neue Technologie" definiert werden.[677]

b. Vorschlag der Art. 29-Gruppe

Trotz dieser ganzen Kriterien und Hinweise, die die DSGVO an die Hand gibt, um feststellen zu können, ob eine DSFA notwendig ist, bleibt die Einschätzung hochgradig subjektiv.[678] Um die Bewertung objektiver zu gestalten, schlägt die Artikel 29-Gruppe ein einfaches Vorgehen vor. Es soll geprüft werden, ob bestimmte Kriterien auf die geplante Verarbeitung zutreffen. Die Kriterien sind:

1. Scoring/Profiling
2. automatisierte Entscheidungsfindung mit Rechtswirkung
3. systematische Überwachung
4. Verarbeitung von besonders sensitiven Daten (vor allem Daten aus Art. 9 DSGVO)
5. umfangreiche Datenverarbeitung (Datenmenge und Anzahl der Betroffenen)
6. Zusammenführung und/oder Abgleich von verschiedenen Datensätzen, wenn Betroffene nicht damit rechnen müssen
7. Verarbeitung von Daten besonders schutzbedürftiger Personengruppen (z.B. Kinder, Kranke)
8. Verwendung neuer Technologien (s. Kapitel J.I.2)
9. Verarbeitung von Daten, die dem Betroffenen die Ausübung seiner Rechte erschwert oder die Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags verhindert (z.B. Bank, die anhand von Auskunfteien darüber entscheidet, ob ein Kredit vergeben wird)

675 *Martini* (2021), Art. 35 Rn. 18; *Baumgartner* (2018), Art. 35 Rn. 1.
676 So auch: *Art.-29-Gruppe*, WP 248, 2017, S. 12.
677 *Martini* (2021), Art. 35 Rn. 18.
678 *Veil*, ZD 2015, S. 347 (352).

Sollten zwei oder mehr dieser Kriterien zutreffen, schlägt die Art. 29-Gruppe vor, dass eine DSFA durchgeführt wird.[679] Der große Vorteil an diesem Vorgehen ist die Einfachheit, mit der die Notwendigkeit einer DSFA festgestellt werden kann.

c. Zwingende Notwendigkeit einer DSFA

In einigen Fällen geht die DSGVO allerdings davon aus, dass intrinsisch ein hohes Risiko vorliegt. Laut Art. 35 Abs. 3 DSGVO ist eine DSFA demnach insbesondere notwendig bei systematischer und umfassender Persönlichkeitsbewertung mit Rechtsfolge, bei umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten i.S.v. Art. 9 Abs. 1 DSGVO und bei systematischer und umfangreicher Überwachung öffentlich zugänglicher Bereiche. Systematisch ist eine Verarbeitung dann, wenn sie planmäßig und strategisch stattfindet.[680] Umfassend und umfangreich ist eine Verarbeitung, wenn sie inhaltlich bzw. räumlich weitgefasst ist und eine große Anzahl von Personen betrifft.[681] Wann die Voraussetzung von ‚systematisch' und ‚umfassend/umfangreich' tatsächlich erfüllt ist, ist wiederum im Einzelfall zu bewerten.[682] Auch muss berücksichtigt werden, dass die Aufzählung aus Art. 35 Abs. 3 DSGVO nicht abschließend, sondern nur beispielhaft ist.

d. Vorgaben der Aufsichtsbehörden

Bei der Einschätzung, ob ein hohes Risiko vorliegt, kommt auch den Aufsichtsbehörden eine wesentliche Rolle zu. Laut Art. 35 Abs. 4 und 5 DSGVO müssen diese Listen veröffentlichen, auf denen Verarbeitungsvorgänge notiert sind, für welche eine DSFA notwendig bzw. nicht notwendig ist. Damit soll Verantwortlichen eine gewisse Rechtssicherheit gegeben werden, wobei die Listen nicht als abschließende Aufzählung gewertet werden sollten.[683]

679 *Art.-29-Gruppe*, WP 248, 2017, S. 7 ff.
680 *Art.-29-Gruppe*, WP 248, 2017, S. 10; *Martini* (2021), Art. 35 Rn. 29a, 31.
681 *Martini* (2021), Art. 35 Rn. 29a, 31.
682 *Baumgartner* (2018), Art. 35 Rn. 36.
683 *Martini* (2021), Art. 35 Rn. 37.

2. Notwendigkeit einer DSFA bei der Verarbeitung von Wesensdaten durch BCI

Laut Art. 35 Abs. 1 DSGVO leitet sich die Notwendigkeit einer DSFA davon ab, ob der Einsatz von neuartigen Technologien und die Art, der Umfang und der Zweck der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen haben könnte.

BCI sind eindeutig als neue Technologie zu definieren, da sie den derzeitigen Stand der Technik im Bereich der Neurotechnologie abbilden. Die Art, der Umfang und der Zweck der Verarbeitung beim Einsatz von BCI wurde bereits ausführlich in Kapitel I.VI.1.a beschrieben. Zusammenfassend kann festgestellt werden, dass Wesensdaten durch BCI in verschiedensten Arten und zu verschiedenen Zwecken verarbeitet werden können. Mit Wesensdaten sind Daten betroffen, die ein noch nie zuvor dagewesenes Auswertungspotential besitzen, auch wenn diese rechtlich nicht zwangsläufig als besondere Kategorien von personenbezogenen Daten einzustufen sind. Da durch BCI in vielen Fällen die Gehirnaktivitäten von einer Vielzahl von Personen ständig und zeitlich unbegrenzt ausgelesen, erhoben und ausgewertet werden müssen, ist die damit einhergehende Verarbeitung auch als entsprechend umfangreich einzustufen.

Allerdings muss der Einsatz der neuen Technologie und die konkrete Verarbeitung auch ein hohes Risiko mit sich bringen, um eine DSFA notwendig zu machen. Dies gilt vor allem dann, wenn die Verarbeitung unter die Aufzählung aus Art. 35 Abs. 3 DSGVO zu fassen ist. Grundlegend kommt dabei lediglich die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten i.S.v. Art. 9 Abs. 1 DSGVO in Frage. Wie in Kapitel G.I.3 bereits dargelegt wurde, ist es allerdings nicht eindeutig, ob Wesensdaten als besondere Kategorien von personenbezogenen Daten definiert werden können. Demnach hängt es von der Rechtsauslegung ab, ob BCI unter Art. 35 Abs. 3 DSGVO subsumiert werden können. Abhängig vom konkreten Einsatz von BCI kann es auch sein, dass eine systematische und umfassende Persönlichkeitsbewertung mit Rechtsfolge vorliegt. In beiden Fällen wäre eine DSFA umgehend notwendig.

Alternativ kann die Verarbeitung von Wesensdaten mit BCI auch auf einer Muss-Liste einer Aufsichtsbehörde enthalten sein. Da diese Listen sich von Bundesland zu Bundesland unterscheiden, kann hier keine abschließende Bewertung präsentiert werden. Tendenziell gilt allerdings, dass die Verarbeitung von Wesensdaten mit BCI, je nach Rechtsauslegung und

konkreter Ausgestaltung, in den meisten Fällen von den Muss-Listen abgedeckt sein dürfte.[684]

Abschließend kann auch das Vorgehen der Art. 29-Gruppe[685] genutzt werden, um festzustellen, ob die Durchführung einer DSFA verpflichtet ist. Hierfür ist es notwendig, zu überprüfen, welche der neun Kriterien zutreffend sind. Grundlegend sind zwei Kriterien uneingeschränkt zutreffend: umfangreiche Datenverarbeitung und Verwendung neuer Technologien. Je nach Rechtsauslegung ist es aber auch zutreffend, dass prinzipiell besondere Kategorien von Daten verarbeitet werden. Allerdings ist es abhängig von der Ausgestaltung der konkreten Verarbeitung auch denkbar, dass noch mehr Kriterien einschlägig sind. BCI können z.B. genutzt werden, um Profiling zu betreiben und um Wesensdaten von besonders schutzbedürftigen Personengruppen zu verarbeiten. Unabhängig davon reichen bereits die zwei grundlegenden und uneingeschränkt zutreffenden Kriterien aus, um eine DSFA notwendig zu machen.[686]

II. Inhalt und Durchführung einer DSFA

Wenn die Schwellenwertanalyse positiv ausfällt, ist es notwendig, eine DSFA tatsächlich durchzuführen. Der zwingend notwendige Mindestinhalt dieser Abschätzung ist in Art. 35 Abs. 7 DSGVO geregelt. Dort werden vier konkrete Punkte genannt:

1. Beschreibung der geplanten Verarbeitung
2. Bewertung der Notwendigkeit und Verhältnismäßigkeit
3. Risikobewertung
4. Abhilfemaßnahmen

Neben diesen Pflichtangaben ist es den Verantwortlichen möglich, weitere individuelle Aspekte in die DSFA miteinzubeziehen, die sich aus dem jeweiligen Einzelfall ergeben.[687]

---

684 Als Vergleich, so z.B. die Muss-Liste der Landesdatenschutzbeauftragten des Landes Niedersachsen: Abrufbar unter: https://lfd.niedersachsen.de/startseite/datenschutzrecht/ds_gvo/liste_von_verarbeitungsvorgangen_nach_art_35_abs_4_ds_gvo/muss-listen-zur-datenschutz-folgenabschatzung-179663.html (aufgerufen 15.1.2023).

685 *Art.-29-Gruppe*, WP 248, 2017, S. 7 ff.

686 Sehen ebenso die grundsätzliche Notwendigkeit einer DSFA bei der Verarbeitung von Wesensdaten: *Ienca/Malgieri,* Journal of Law and the Biosciences 2022, S. 1 (15).

687 *Baumgartner* (2018), Art. 35 Rn. 48.

1. Beschreibung der geplanten Verarbeitung

Grundlegend für die DSFA verlangt Art. 35 Abs. 7 lit. a DSGVO die systematische Beschreibung der geplanten Verarbeitung, bei der die Zwecke der Verarbeitung genau dargelegt werden müssen. Sobald die Verarbeitung auf einem berechtigten Interesse fußt, ist dieses ebenso anzugeben. Inhaltlich sollte sich die Beschreibung an den Vorgaben aus Art. 30 Abs. 1 DSGVO[688] orientieren.[689] Demnach müssen vor allem der Verantwortliche, die Zwecke und Rechtsgrundlagen der Verarbeitung, die Kategorien der betroffenen Personen und personenbezogenen Daten, die Empfänger der Daten (z.B. eingesetzte IT-Systeme, Auftragsverarbeiter), vorhandene Drittlandtransfers, Löschfristen und allgemeine technische und organisatorische Maßnahmen systematisch beschrieben werden.

2. Bewertung der Notwendigkeit und Verhältnismäßigkeit

Anhand der systematischen Beschreibung der geplanten Verarbeitung soll der Verantwortliche dann sorgfältig bewerten, ob die Verarbeitung tatsächlich notwendig und in der Umsetzung auch verhältnismäßig ist. Maßgeblich sind dabei die Zweckbindung und Datenminimierung aus Art. 5 DSGVO.[690] Der Verantwortliche muss die Notwendigkeit nachweisen, indem dieser schlüssig darlegt, dass der Zweck nur mit der Datenverarbeitung ganzheitlich erreicht werden kann.[691] Dabei ist auch aufzuzeigen, dass die Daten bei der geplanten Verarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind.[692] Die Verhältnismäßigkeit ist wiederum nachzuweisen, indem beschrieben wird, dass die eingesetzten Mittel tatsächlich sinnvollerweise dazu geeignet sind, den Zweck zu erreichen.[693]

688 Enthält Vorgaben zum Inhalt des Verzeichnisses von Verarbeitungstätigkeiten.
689 *Laue* (2019), Art. 35 DSGVO Rn. 24; *Baumgartner* (2018), Art. 35 Rn. 51; *Martini* (2021), Art. 35 Rn. 47.
690 *Baumgartner* (2018), Art. 35 Rn. 52.
691 *Laue* (2019), Art. 35 DSGVO Rn. 26; *Martini* (2021), Art. 35 Rn. 48.
692 *Martini* (2021), Art. 35 Rn. 48.
693 *Laue* (2019), Art. 35 DSGVO Rn. 26.

3. Risikobewertung

Auf die Bewertung der Notwendigkeit und auf die Verhältnismäßigkeitsprüfung baut die ausführliche Risikobewertung auf. Diese knüpft an das ggf. bereits festgestellte hohe Risiko an, welches bei der anfänglichen Schwellenwertanalyse eine DSFA notwendig gemacht hat und legt dieses ausführlicher dar.[694] Ziel dabei ist es, zu überprüfen, ob das hohe Risiko für die Rechte und Freiheiten der Betroffenen auch tatsächlich vorliegt und ob sich jenes mit den Interessen der Verantwortlichen angemessen vereinbaren lässt.[695] Gemäß ErwG. 90 gilt es auch hier, die mögliche Schadensauswirkung für betroffene Personen und die Eintrittswahrscheinlichkeit des jeweiligen Schadens ins Zentrum zu stellen.[696] Bei der Bewertung der Eintrittswahrscheinlichkeit sind interne wie auch externe Faktoren/Verursacher zu berücksichtigen.[697] Die Analyse der beiden grundlegenden Risikobewertungs-Faktoren soll dann eine Einstufung in eine Risikolasse („normal", „hoch", „sehr hoch") ermöglichen.[698] Aus der Risikoklasse ergibt sich das tatsächliche Risiko, welches dann den konkreten Schutzbedarf bestimmt.[699]

4. Abhilfemaßnahmen

Entsprechend dem abgeleiteten Schutzbedarf sollen Abhilfemaßnahmen ergriffen werden, die dazu geeignet sind, das Risiko einzudämmen.[700] Das bedeutet, dass die Maßnahmen in der Lage sein sollen, das festgestellte hohe Risiko unter das Bedenklichkeitsniveau abzusenken und den Schutz der personenbezogenen Daten vor den möglichen Schäden zu gewährleisten.[701] Wie in Art. 4 Nr. 12 DSGVO dargelegt, bedeutet dies, die Daten vor unbeabsichtigter und unrechtmäßiger Vernichtung, Verlust, Veränderung, Offenlegung oder Zugänglichkeit zu schützen.

694 *Baumgartner* (2018), Art. 35 Rn. 53; *Laue* (2019), Art. 35 DSGVO Rn. 27.
695 *Martini* (2021), Art. 35 Rn. 51; *Laue* (2019), Art. 35 DSGVO Rn. 27.
696 *Art.-29-Gruppe*, WP 248, 2017, S. 17.
697 *Laue* (2019), Art. 35 DSGVO Rn. 27; *Martini* (2021), Art. 35 Rn. 52; *Hansen* (2020), Art. 35 Rn. 47.
698 *Laue* (2019), Art. 35 DSGVO Rn. 27; *Martini* (2021), Art. 35 Rn. 52.
699 *Jandt* (2020), Art. 35 Rn. 45; *Laue* (2019), Art. 35 DSGVO Rn. 27.
700 *Martini* (2021), Art. 35 Rn. 54; *Baumgartner* (2018), Art. 35 Rn. 53 f.
701 *Baumgartner* (2018), Art. 35 Rn. 56; *Martini* (2021), Art. 35 Rn. 54.

Als geeignete Abhilfemaßnahmen benennt Art. 35 Abs. 7 lit. d DSGVO explizit Garantien, Sicherheitsvorkehrungen und Verfahren. Allerdings werden diese Begriffe nicht weiter erklärt oder voneinander abgegrenzt.[702] Naheliegend ist allerdings, dass die in Art. 32 Abs. 1 lit. a-d DSGVO geforderten technischen und organisatorischen Maßnahmen herangezogen werden können.[703] Ergänzend dazu sind weitere risikomindernde Maßnahmen denkbar (z.B. vertragliche Maßnahmen oder transparente Kommunikation mit Betroffenen).[704] Die geplanten Abhilfemaßnahmen müssen dokumentiert werden, indem die Maßnahmen den jeweiligen Risiken und Schutzzielen zugeordnet und mögliche Restrisiken transparent gemacht werden.[705]

5. Ergebnis der DSFA

Aus der DSFA soll hervorgehen, wie das hohe Risiko mithilfe von Abhilfemaßnahmen auf ein vertretbares Niveau abgemildert wird. Sollte bei der Beurteilung festgestellt werden, dass das Risiko nicht ausreichend minimiert werden kann, muss gemäß Art. 36 DSGVO die zuständige Aufsichtsbehörde konsolidiert werden.[706]

Vom Ergebnis kann auch abhängig gemacht werden, in welchem Abstand die DSFA wieder überprüft werden muss. Gemäß Art. 35 Abs. 11 DSGVO ist der Verantwortliche dazu verpflichtet, zu prüfen, ob die Angaben in der DSFA und die zugrundeliegenden Annahmen weiterhin korrekt sind.[707] Je höher das Risiko, umso regelmäßiger ist eine Überprüfung der Ergebnisse vorzunehmen.[708]

6. Datenschutz-Folgeabschätzung bei BCI

Wie bereits festgestellt wurde, wird bei der Verarbeitung von Wesensdaten durch BCI für gewöhnlich die Durchführung einer DSFA notwendig

702 *Baumgartner* (2018), Art. 35 Rn. 54.
703 *Laue* (2019), Art. 35 DSGVO Rn. 29; *Baumgartner* (2018), Art. 35 Rn. 55; *Martini* (2021), Art. 35 Rn. 54.
704 *Jandt* (2020), Art. 35 Rn. 49; *Hansen* (2020), Art. 35 Rn. 48; *Baumgartner* (2018), Art. 35 Rn. 55; *Laue* (2019), Art. 35 DSGVO Rn. 29.
705 *Hansen* (2020), Art. 35 Rn. 49; *Baumgartner* (2018), Art. 35 Rn. 57.
706 *Baumgartner* (2018), Art. 36 Rn. 8 f.
707 *Martini* (2021), Art. 35 Rn. 72.
708 *Baumgartner* (2018), Art. 35 Rn. 77.

sein. Der Inhalt der DSFA ist vom jeweiligen konkreten Verarbeitungsfall abhängig. Hier soll allerdings an einem bestimmten Fall aufgezeigt werden, wie die Durchführung einer DSFA für die Verarbeitung von Wesensdaten durch BCI aussehen könnte. Hierfür soll ein urtümlicher Anwendungsfall für BCIs als Grundlage dienen, nämlich die Steuerung von Unterstützungsrobotern per BCI.

a. Beschreibung der geplanten Verarbeitung

Verarbeitungszweck

Zweck der Verarbeitung ist die Steuerung von Hilfs- und Unterstützungsrobotern per BCI durch beeinträchtigte Menschen.

Rechtsgrundlage

Als Rechtsgrundlage für die Verarbeitung dient die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO.

Kategorie betroffener personenbezogener Daten

Bei der Verarbeitung sind folgende personenbezogene Daten betroffen:

- Name
- Kontaktdaten
- Adressdaten
- Zahlungsdaten
- Wesensdaten

Kategorie betroffener Personen

Betroffen von der Datenverarbeitung sind alle Nutzer der Technologie und des Dienstes.

Werden Auftragsverarbeiter eingesetzt? (inkl. Nennung)

Im konkreten Fall müssten hier alle Auftragsverarbeiter aufgelistet werden.

In diesem Beispiel ist es denkbar, dass der Verantwortliche einen Cloud-Anbieter nutzt, um die Daten zu speichern.

Findet eine Übermittlung an ein Drittland oder eine internationale Organisation statt?

Im konkreten Fall müsste unter diesem Punkt aufgelistet werden, ob und wohin Daten an ein Drittland oder eine internationale Organisation übermittelt werden.

In dem hier betrachteten Anwendungsfall ist es z.B. denkbar, dass der Verantwortliche einen Cloud-Anbieter nutzt, der in den USA sesshaft ist.

Gibt es weitere relevante Normen, Standards, Zertifizierungen und Verhaltensregeln?

Im konkreten Fall müsste hier Entsprechendes aufgelistet werden.

In dem betrachteten Beispiel gibt es keine weiteren relevanten Normen, Standards, Zertifizierungen und/oder Verhaltensregeln.

Standpunkt der Betroffenen (Art. 35 Abs. 9 DSGVO)

Der Standpunkt der betroffenen Personen wurde nicht eingeholt. Grund ist der dafür notwendige, unangemessen hohe Aufwand.

Lebenszyklus der Daten

Das Nutzerprofil (Name, Kontaktdaten, Adressdaten und Zahlungsdaten) wird bei Inbetriebnahme erstellt und solange gespeichert, bis die Nutzung langfristig eingestellt wird (nach 12 Monate Inaktivität) oder, wenn der Nutzer seine Einwilligung widerruft.

Die Wesensdaten werden bei jeder Nutzung der Technologie mit der entsprechenden Anwendung erhoben. Nach der Erhebung werden die Daten ausgewertet und in entsprechende Befehle für die Hilfs-/Unterstützungsroboter übersetzt. Die Rohdaten und entsprechenden Befehle werden gesammelt und ausgewertet, um die Technologie und Anwendung auf den Nutzer abzustimmen und kontinuierlich zu verbessern. Erst bei Löschung des Nutzerkontos oder der endgültigen Einstellung der Nutzung (nach 12 Monaten Inaktivität) werden die Wesensdaten vollständig gelöscht.

Welche Betriebsmittel werden eingesetzt?

Im konkreten Fall müsste unter diesem Punkt aufgelistet werden, welche konkreten Betriebsmittel eingesetzt werden.

In dem hier betrachteten Anwendungsfall ist es z.B. denkbar, dass der Verantwortliche diverse Softwareanwendung zum Cloud-Hosting, Monitoring und als Backend nutzt.

b. Bewertung der Notwendigkeit und Verhältnismäßigkeit

Warum ist die Verarbeitung zwingend erforderlich?

Ohne BCI und die entsprechende Anwendung wäre es für die beeinträchtigten Nutzer nicht möglich, Hilfs-/Unterstützungsroboter in derselben Weise zu steuern. Demnach ist die Verarbeitung zwingend erforderlich, um den Verarbeitungszweck zu erreichen.

Sind die Daten für die Verarbeitung zwingend erforderlich?

Ohne Name, Kontaktdaten, Adressdaten und Kontodaten wäre es nicht möglich, das Nutzerkonto zu erstellen.

Ohne die Verarbeitung von Wesensdaten wäre ebenso keine Steuerung der Roboter per neurologischem Signal möglich. Die Daten sind demnach zwingend erforderlich, um den Verarbeitungszweck zu erfüllen.

Warum ist die Verarbeitung verhältnismäßig?

Die Verarbeitung von Wesensdaten ist zwingend erforderlich, um den Zweck zu erreichen. Ohne BCI und einer entsprechenden Anwendung, wäre es überhaupt nicht möglich die Wesensdaten zu verarbeiten. Demnach sind auch die eingesetzten Mittel sinnvollerweise dazu geeignet, um den Zweck zu erreichen.

Wie werden die Daten korrekt und auf dem neusten Stand gehalten?

Die zur Zweckerreichung notwendigen Wesensdaten werden bei jeder Nutzung der Technologie und der Anwendung kontinuierlich aktuell erhoben. Die Daten sind demnach automatisch immer auf dem neuesten Stand.

Die Korrektheit der Daten wird durch den Übersetzungsalgorithmus gewährleistet, der die Rohdaten in entsprechende Befehle übersetzt. Der Übersetzungsalgorithmus wird ständig weiterentwickelt und mithilfe von Nutzerdaten kontinuierlich verbessert. Ebenso wird die Sicherheit der Software regelmäßig durch externe Audits überprüft.

Welche Speicherdauer haben die Daten?

Das Profil und die Wesensdaten werden bei Löschung des Nutzerkontos oder endgültiger Einstellung der Nutzung (nach 12 Monaten Inaktivität) vollständig gelöscht.

c. Risikobewertung[709]

Bei der Risikobewertung hat sich in der Praxis der Einsatz einer Risikomatrix (Tabelle 1) durchgesetzt. In dieser wird die Eintrittswahrscheinlichkeit der Schadensauswirkung gegenübergesetzt. Beide Kriterien werden mit einer Ziffer von 1-4 bewertet und ergeben in Verbindung einen Risikowert.

Eintrittswahrscheinlichkeit	fast sicher	4	8	12	16
	wahrscheinlich	3	6	9	12
	eher selten	2	4	6	8
	unwahrscheinlich	1	2	3	4
		unkritisch	beeinträchtigend	kritisch	katastrophal
		Schadensauswirkung			

Tabelle 1: Risikomatrix

Der durch die Risikomatrix erhaltene Risikowert kann dann in eine Risikoklasse übertragen werden. Gemäß der Risikoklasse ergeben sich dann Maßnahmen, die vom Verantwortlichen umgesetzt werden müssen.

von	bis	Risikoklasse	Maßnahme
1	2	C (keine Gefährdung)	Gelegentliche Überprüfung der DSFA – ansonsten keine besonderen Maßnahmen notwendig
3	7	B (vertretbares Risiko)	Ständige Überwachung des Risikos und regelmäßige Überprüfung der DSFA
8	16	A (nicht vertretbares Risiko)	Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO

Tabelle 2: Übersicht der Risikoklassen

Anhand dieser Systematik sollen nachfolgend relevante Risiken bei der Verarbeitung von Wesensdaten durch BCI mit dem Zweck der Steuerung von Hilfs-/Unterstützungsroboter analysiert und bewertet werden.

709 Bei der Risikobewertung wurde sich an die Empfehlungen des Bayerischen Landesbeauftragten für den Datenschutz (BayLfD) orientiert: Abrufbar unter: https://www.datenschutz-bayern.de/dsfa/ (abgerufen 5.3.2023).

Dabei werden auch direkt explizite Abhilfemaßnahmen für die jeweiligen Risiken benannt. Unter Berücksichtigung der Abhilfemaßnahmen wird dann eine abschließende Einordnung in eine Risikoklasse vorgenommen, die wiederum jeweils mit entsprechenden Maßnahmen einhergeht.

Ziel *	Schwachstelle	Risikoquelle	Risikoszenario	Eintrittswahrscheinlichkeit		Schadensauswirkung		Risikowert/-klasse	Abhilfemaßnahmen	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Wert	Erläuterung	Wert			Erläuterung	Risikoklasse
Verf.	**Ressourcenausfall** Notwendiges Personal und Know-how steht nicht zur Verfügung	Personal	Fehlendes Personal kann nicht kurzfristig ersetzt werden, was dazu führt, dass technisch notwendige Prozesse und Incident-Tickets ggf. nicht ausreichend betreut und bearbeitet werden können.	Um die Verf. der BCI und der Anwendung zu gewährleisten, bedarf es hochspezialisierter Fachkräfte mit Spezial-Know-how. Erfahrungsgemäß kann kurzfristiger Personalausfall zu Verzögerungen führen.	3	Falls bspw. beeinträchtigte Nutzer nicht mehr ihre Hilfs-/ Unterstützungsroboter steuern können, kann dies zu ernsthaften Einbußen in der Lebensqualität dieser Menschen führen.	4	12/A	Single-points-of-failure reduzieren (mehr Schulungen für Mitarbeiter (MA) = mehr MA mit Know-how)	Mit den Abhilfemaßnahmen kann das Risiko eingedämmt werden. Allerdings kann die inhärente Dynamik in der Personalplanung nicht vollkommen beseitigt werden.	B
									Ständige Überwachung der Personalentwicklung (schnellere Reaktion bei Ausfall)		
									Outsourcing: Es können kurzfristig die Dienstleistungen von Freelancern in Anspruch genommen werden.		
									Automatisierung: So viele Prozesse wie möglich MA-unabhängig gestalten		

									Es werden regelmäßige Backups durchgeführt und mehrfach gesichert.		
Ziel *	**Schwachstelle**	**Risikoquelle**	**Risikoszenario**	**Eintrittswahrscheinlichkeit**		**Schadensauswirkung**		**Risikowert/-klasse**	**Abhilfemaßnahmen**	**Risikoeinschätzung mit Maßnahmen**	
				Erläuterung	**Wert**	**Erläuterung**	**Wert**			**Erläuterung**	**Risikoklasse**
Verf.	**Ressourcenausfall** Notwendige Hardware steht nicht zur Verfügung	Technik	Fehlerhafte Hardware kann nicht kurzfristig ersetzt werden, was dazu führt, dass die Anwendung nicht verfügbar ist und/oder Daten verloren gehen.	Um die Verf. der Anwendung zu gewährleisten, bedarf es hochspezialisierter Hardware (Server, Switche etc.). Erfahrungsgemäß kann Hardware verschleißen und ausfallen.	3	Falls bspw. beeinträchtigte Nutzer nicht mehr ihre Hilfs-/ Unterstützungsroboter steuern können, kann dies zu ernsthaften Einbußen in der Lebensqualität dieser Menschen führen.	4	12/A	In den Service-Level-Agreements wird eine realistische, auf Erfahrungswerten basierende Verfügbarkeitsquote angegeben. Mit den Herstellern der Hardware wurden Wartungsverträge abgeschlossen, die feste Reaktionszeiten beinhalten. Gängige und leicht verfügbare Hardware (z.B. Kabel, Switche u.Ä.) wird auf Vorrat gehalten.	Mit den Abhilfemaßnahmen kann das Risiko maßgeblich eingedämmt werden.	C

Ziel *	Schwachstelle	Risikoquelle	Risikoszenario	Eintrittswahrscheinlichkeit		Schadensauswirkung		Risikowert/-klasse	Abhilfemaßnahmen	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Wert	Erläuterung	Wert			Erläuterung	Risikoklasse
									Die Anwendung wird redundant in einem anderen Rechenzentrum betrieben. Es werden regelmäßige Backups durchgeführt und mehrfach gesichert. Automatisierung: So viele Prozesse wie möglich MA-unabhängig gestalten		
Verf.	**Überlastung** Es könnte eine Überlastung des Systems hervorgerufen werden.	Dritte	Dritte könnten die Anwendung mit DoS (Denial-of-Service)- und/oder DDoS (Distributed-Denial-of-Service)-Angriffen überlasten.	Böswillige Dritte könnten Interesse daran, haben den Verantwortlichen mit Überlastungen zu erpressen.	2	Falls bspw. beeinträchtigte Nutzer nicht mehr ihre Hilfs-/ Unterstützungsroboter steuern können, kann dies zu ernsthaften Einbußen in der Lebensqualität	4	8/B	Überwachung der Kommunikation auf böswilligen Traffic Anfragen werden priorisiert Die Anwendung wird redundant in einem ande-	Mit den Abhilfemaßnahmen kann das Risiko maßgeblich eingedämmt werden.	C

						dieser Menschen führen.			ren Rechenzentrum betrieben. Es werden regelmäßige Backups durchgeführt und mehrfach gesichert.		
Ziel *	**Schwachstelle**	**Risikoquelle**	**Risikoszenario**	**Eintrittswahrscheinlichkeit**		**Schadensauswirkung**		**Risikowert/-klasse**	**Abhilfemaßnahmen**	**Risikoeinschätzung mit Maßnahmen**	
				Erläuterung	**Wert**	**Erläuterung**	**Wert**			**Erläuterung**	**Risikoklasse**
Vert.	**Unbefugter Zugang** Es könnte unbefugter Zugang zu den Daten erhalten werden.	Personal, Dritte	Durch unklare Berechtigungen könnten unbefugte Mitarbeiter Zugriff auf die Daten bekommen.	Die Bereitstellung der Anwendung ist hoch komplex und bedarf der Mitwirkung vieler unterschiedlicher Mitarbeiter.	3	Betroffene Benutzer könnten Opfer von Identitätsdiebstahl, Erpressung und Betrug werden.	4	12/A	Berechtigungs- und Zugangskonzepte werden kontinuierlich auf Aktualität und Sinnhaftigkeit überprüft.	Mit den Abhilfemaßnahmen kann das Risiko weitestgehend eingedämmt werden, da damit ein unbefugter Zugang deutlich erschwert wird und die Daten nur noch bedingt eine Verknüpfung zu einer bestimmten Person zulassen.	B
			Durch Hacking könnten böswillige Dritte unbefugten Zugang zu den Daten bekommen.	Die verarbeiteten Daten haben ein hohes Informationsschöpfungspotential und sind entsprechend interessant für böswillige Dritte.					Mitarbeiter/Benutzer bekommen nur nach einer sicheren Authentifizierung (2-Faktor-Auth.) Zugriff auf die Daten. Mitarbeiter werden regelmäßig zu IT-Sicherheitsthemen geschult und durch		

									interne Richtlinien verpflichtet.		
									Die Übermittlung der Daten wird durch eine aktuelle und sichere Verschlüsselung geschützt.		
									Die Kommunikation mit den BCIs wird mit einer state-of-the-art Firewall gesichert.		
									Die Daten werden weitestgehend pseudonymisiert oder anonymisiert.		
									Es werden nur die Daten erhoben und verarbeitet, die für den Zweck zwingend notwendig sind.		

Ziel *	Schwachstelle	Risikoquelle	Risikoszenario	Eintrittswahrscheinlichkeit		Schadensauswirkung		Risikowert/-klasse	Abhilfemaßnahmen	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Wert	Erläuterung	Wert			Erläuterung	Risikoklasse
Int.	**Unbefugte Veränderung** Es könnten unbefugte Veränderungen an den Daten vorgenommen werden.	Personal, Dritte	Durch unklare Berechtigungen könnten unbefugte Mitarbeiter Daten bewusst/unbewusst verändern.	Die Bereitstellung der Anwendung ist hoch komplex und bedarf der Mitwirkung vieler unterschiedlicher Mitarbeiter.	2	Betroffene Benutzer könnten die Kontrolle über ihre Hilfs-/ Unterstützungsroboter verlieren.	4	8/B	Berechtigungs- und Zugangskonzepte werden kontinuierlich auf Aktualität und Sinnhaftigkeit überprüft.	Mit den Abhilfemaßnahmen kann das Risiko maßgeblich eingedämmt werden. Der Zugang zur Kommunikation, zu den Nutzerkonten und Nutzerdaten wird weitestgehend abgesichert. Eine Veränderung von Daten wird damit deutlich erschwert.	C
			Durch Hacking könnten böswillige Dritte unbefugte Veränderungen an den Daten vornehmen.	Mit einer Veränderung der Daten/Befehle könnten böswillige Dritte die Kontrolle über die Hilfs-/ Unterstützungsroboter übernehmen – allerdings nur in Einzelfällen denkbar und nicht großflächig.					Mitarbeiter/ Benutzer bekommen nur nach einer sicheren Authentifizierung (2-Faktor-Auth.) Zugriff auf die Daten.		
									Mitarbeiter werden regelmäßig zu IT-Sicherheitsthemen geschult und durch interne Richtlinie verpflichtet.		
									Die Übermittlung der Daten wird durch eine aktuelle und si-		

									chere Verschlüsselung geschützt.		
									Die Kommunikation mit den BCIs wird mit einer state-of-the-art Firewall gesichert.		

* IT-Schutzziele: Verfügbarkeit (Verf.), Vertraulichkeit (Vert.), Integrität (Int.)

d. Ergebnis einer DSFA bei der Verarbeitung von Wesensdaten

Das Ergebnis einer DSFA hängt im Einzelfall immer von den vorhandenen Möglichkeiten und der konkreten Argumentation der durchführenden Partei ab. Vorausgehend konnte beispielhaft gezeigt werden, wie eine solche Argumentation bei der Verarbeitung von Wesensdaten in Zukunft aussehen könnte. Grundsätzlich ist es demnach möglich, das inhärent hohe Risiko, welches bei der Datenverarbeitung durch BCI vorliegt, durch umfangreiche und spezielle Abhilfemaßnahmen soweit abzumildern, dass eine Durchführung der geplanten Verarbeitung vertretbar ist.

K. Grundsätze der Verarbeitung

I. Analyse von Art. 5 DSGVO

Die DSGVO legt in Art. 5 einige Grundsätze dar, die bei der Verarbeitung von personenbezogenen Daten grundsätzlich zu berücksichtigen sind. Da bereits dargelegt wurde, dass es sich bei Wesensdaten um personenbezogene Daten handelt, gelten diese auch bei der Verarbeitung mittels BCI. In diesem Kapitel sollen diese Grundsätze somit abschließend betrachtet und auf BCI angewandt werden.

Besonders dabei ist, dass diese Grundsätze objektiv gelten, und in weiteren Artikeln der DSGVO aufgegriffen und konkretisiert werden, aber auch unabhängig von diesen den Verantwortlichen generell zur Einhaltung verpflichten.[710] Da Art. 5 DSGVO eine zentrale Rolle im Datenschutzrecht einnimmt und etliche weitere Vorschriften der DSGVO diese dort normierten Grundsätze aufgreifen, ist jeweils eine einführende Analyse notwendig, um eine Grundlage für die weitere Betrachtung zu gewährleisten.

In Art. 5 Abs. 1 DSGVO werden 6 verschiedene Grundsätze benannt und abstrakt definiert. Dabei handelt es sich konkret um Rechtmäßigkeit/Verarbeitung nach Treu und Glauben/Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit.

1. Art. 5 Abs. 1 lit. a DSGVO: Rechtmäßigkeit/Verarbeitung nach Treu und Glauben/Transparenz

a. Rechtmäßigkeit

Dem Rechtmäßigkeitsgebot kann entweder ein weites oder enges Verständnis zugrunde gelegt werden.[711] Das enge Verständnis ergibt sich aus Art. 8 Abs. 2 GRCh und ErwG. 40, worin eine zweckgebundene Datenverarbeitung auf Grundlage einer Einwilligung oder sonstiger legitimer Rechts-

710 *Herbst* (2020), Art. 5 Rn. 1.
711 *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 4.

grundlage (bspw. zulässiges Mitgliedsstaatenrecht) gefordert wird.[712] Daraus lässt sich ableiten, dass sich die Rechtmäßigkeit vor allem aus den Rechtmäßigkeitsvoraussetzungen nach Art. 6 Abs. 1 DSGVO[713] oder Art. 9 Abs. 2 DSGVO ergibt. Im Gegensatz dazu wird beim weiten Verständnis davon ausgegangen, dass nicht nur eine Rechtsgrundlage gemäß Art. 6 Abs. 1 UAbs. 1 DSGVO vorliegen muss, sondern auch alle zusätzlichen Anforderungen und Pflichten, die sich aus der DSGVO oder sonstigem legitimen Recht ergeben, einzuhalten sind, damit die Rechtmäßigkeit nach Art. 5 Abs. 1 lit. a DSGVO erfüllt ist.[714]

Mit dem weiten Verständnis gehen jedoch erhebliche Abgrenzungsschwierigkeiten einher, die dazu führen würden, dass jeglicher Verstoß gegen die DSGVO immer auch ein Verstoß gegen den zentralen Grundsatz der Rechtmäßigkeit darstellen würde.[715] Um eine trennscharfe Betrachtung zu gewährleisten und um den Rahmen nicht zu sprengen, wird in dieser Arbeit demnach der engen Auslegung gefolgt, womit die Rechtmäßigkeit gemäß Art. 5 Abs. 1 lit. a DSGVO sich insbesondere aus einer der Rechtsgrundlagen aus Art. 6 Abs. 1 UAbs. 1 oder Art. 9 Abs. 2 DSGVO ergibt.

b. Verarbeitung nach Treu und Glauben

Die von der DSGVO verwendete Formulierung „nach Treu und Glauben" ist nicht identisch mit dem gleichnamigen deutschen zivilrechtlichen Grundsatz nach § 242 BGB.[716] Auf Grundlage der englischen Version der DSGVO, die das Wort „fairly" benutzt, ist vielmehr davon auszugehen, dass grundsätzlich eine „faire" Verarbeitung gefordert wird.[717] Unabhängig von der genauen Terminologie bleibt dieser Grundsatz der Verarbeitung aber uneindeutig und lässt sich nur sehr schwierig von den anderen Grundsätzen aus Art. 5 Abs. 1 DSGVO abgrenzen.[718] Es ist davon auszugehen, dass die Verarbeitung nach Treu und Glauben bzw. die faire Verarbeitung vielmehr einen Auffangtatbestand darstellt, der von betroffenen Personen

712 *Herbst* (2020), Art. 5 Rn. 8 u. 10; *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 4.
713 *Herbst* (2020), Art. 5 Rn. 8.
714 *Roßnagel* (2019), Art. 5 Rn. 32.
715 *Herbst* (2020), Art. 5 Rn. 10.
716 *Frenzel* (2021) BDSG, Art. 5 Rn. 19; *Herbst* (2020), Art. 5 Rn. 13.
717 *Reimer* (2018), Art. 5 Rn. 14; *Frenzel* (2021) BDSG, Art. 5 Rn. 18.
718 *Pötters* (2018), Art. 5 Rn.9; *Herbst* (2020), Art. 5 Rn. 13-17; *Roßnagel* (2019), Art. 5 Rn. 45.

auch bei unklaren zu beanstandenden Verarbeitungen als Generalklausel herbeigezogen werden kann, um das Kräftegleichgewicht zwischen Verantwortlichen und Betroffenen zu erhalten.[719] Ein Verstoß gegen das Fairnessgebot liegt meistens dann vor, wenn die vernünftige Erwartungshaltung der Betroffenen verletzt[720] oder deren Vertrauen missbraucht wurde.[721] Die Erwartungshaltung ist z.B. besonders bei einer Interessenabwägung zu Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zu berücksichtigen.[722] Ein Vertrauensmissbrauch könnte wiederrum darin gesehen werden, wenn eine Einwilligung von der betroffenen Person eingeholt wird, obwohl die Datenverarbeitung gleichzeitig bereits durch eine andere Rechtsgrundlage erlaubt ist, womit dem Betroffenen irrtümlich weisgemacht wird, er hätte ein Widerspruchsrecht gemäß Art. 7 Abs. 3 S. 2 DSGVO.[723]

c. Transparenz

Ein wesentlicher Grundpfeiler des modernen Datenschutzrechts ist das Transparenzgebot, da Betroffene das Risiko einer Verarbeitung ihrer personenbezogenen Daten nur einschätzen können, wenn diese in einer für sie nachvollziehbaren Weise stattfindet.[724] Wie genau eine solche Transparenz für die Betroffenen hergestellt werden soll, beschreibt ErwG 39. Laut ErwG. 39 S. 2, 4 und 5 sind insbesondere die Art der Daten, die Art der Verarbeitung, der Umfang der Verarbeitung, die Identität des Verantwortlichen, der Zweck der Datenverarbeitung, die Rechte der Betroffenen (insb. deren Auskunftsrecht) und die Risiken, Vorschriften, Garantien und Rechte, die im Zusammenhang mit der Verarbeitung stehen, offenzulegen. Ebenso ist darzulegen, wie diesbezügliche Rechte geltend gemacht werden können. In ErwG. 39 S. 3 wird konkretisiert, dass die Informationen und Mitteilungen leicht zugänglich und verständlich und in klarer und einfacher Sprache verfasst sein müssen. Weiterhin ergänzt ErwG. 39 S. 2, dass diese Transparenzvorschriften auch für künftige Verarbeitungen gelten. Eine tiefergehende Konkretisierung dieses Transparenzgebotes findet sich in Art. 12, 13, 14, 15 DSGVO.

719 *Herbst* (2020), Art. 5 Rn. 17.
720 *Heberlein* (2018), Art. 5 Rn. 10.
721 *Roßnagel* (2019), Art. 5 Rn. 47.
722 *Heberlein* (2018), Art. 5 Rn. 10.
723 *Roßnagel* (2019), Art. 5 Rn. 47.
724 *Pötters* (2018), Art. 5 Rn. 11.

Grundsätzlich sind der betroffenen Person demnach alle Informationen über die Verarbeitung ihrer Daten zur Verfügung zu stellen, damit diese das Risiko der Verarbeitung einschätzen und ggf. Maßnahmen ergreifen kann. Demnach ist insbesondere eine heimliche Verarbeitung von Daten ausgeschlossen.[725]

2. Rechtmäßigkeit/Verarbeitung nach Treu und Glauben/Transparenz bei Wesensdaten

a. Rechtmäßigkeit bei der Verarbeitung von Wesensdaten

Wie in Kapitel G.II gezeigt wurde, kann die Verarbeitung von Wesensdaten mittels BCI über mehrere Rechtmäßigkeitsvoraussetzungen aus Art. 6 Abs.1 DSGVO legitimiert werden. Vorrangig ist dabei die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO anzuführen. Solange die Vorgaben an die Freiwilligkeit, Transparenz, Zweckbindung und Form erfüllt sind, kann davon ausgegangen werden, dass die betroffene Person die mit der Verarbeitung von Wesensdaten einhergehenden Risiken ausreichend abschätzen und somit eine selbstbestimmte Entscheidung treffen kann. Neben der Einwilligung ist es ebenso denkbar, dass das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO herangezogen wird. Es gibt Möglichkeiten, die Verarbeitung von Wesensdaten über das berechtigte Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zu rechtfertigen. Dies stellt kein Problem dar, solange Verantwortliche gewissenhaft die notwendigen Interessenabwägungen durchführen und sich an die festgelegten Zwecke der Datenverarbeitung halten. Zu guter Letzt ist es auch denkbar, dass Wesensdaten in Zukunft aufgrund bestimmter Verträge gemäß Art. 6 Abs. 1 lit. b DSGVO verarbeitet werden könnten.

Inwiefern die Rechtmäßigkeitsvoraussetzungen nach Art. 9 Abs. 2 DSGVO relevant sind, ist im Bezug auf Wesensdaten derzeit noch unklar. Wie in Kapitel G.I.3.d beschrieben wurde, ist allerdings davon auszugehen, dass diese in der Praxis häufig nicht im Geltungsbereich von Art. 9 DSGVO verortet werden dürften.

725 *Herbst* (2020), Art. 5 Rn. 18.

b. Treu und Glauben bei der Verarbeitung von Wesensdaten

In Kapitel G.II.6.c wurde beschrieben, wie eine Interessenabwägung zu Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO vorgenommen werden könnte, um die Verarbeitung von Wesensdaten zu legitimieren. Diese Abwägung war nur beispielhaft und könnte durchaus als unfair bezeichnet werden. Die Erfahrungen aus der Praxis zeigen auch, dass dies häufig der Fall ist, wenn das berechtigte Interesse als Rechtsgrundlage herangezogen wird. Es ist also davon auszugehen, dass das berechtigte Interesse auch in Bezug auf Wesensdaten als Auffangklausel ausgenutzt werden könnte, um umfangreichere und sensitivere Auswertungen von Wesensdaten, die nicht mit einer Einwilligung oder mithilfe eines zugrundeliegenden Vertrags gerechtfertigt werden können, scheinbar zu legitimieren. Um dem Grundsatz von Treu und Glauben gerecht zu werden, ist dies in Zukunft zu vermeiden. Am besten wäre dies möglich, wenn Wesensdaten prinzipiell unter den besonderen Schutz von Art. 9 DSGVO fallen würden. Damit würde das berechtigte Interesse als valide Rechtsgrundlage ausgeschlossen werden, womit eine unnötig umfangreiche Verarbeitung von Wesensdaten vermieden wird.

c. Transparenz bei der Verarbeitung von Wesensdaten

Bezüglich der Transparenz wurde in dieser Arbeit besonders Art. 15 DSGVO betrachtet. Das Auskunftsrecht ist ein zentrales Mittel, um der betroffenen Person Einblick in die Verarbeitung ihrer Daten zu verschaffen. Es wurde bereits dargelegt, wie eine solche Auskunft bei der Verarbeitung von Wesensdaten mittels BCI in Zukunft aussehen könnte.

Neben Art. 15 DSGVO müssen Verantwortliche, die Daten mit Neurotechnologien verarbeiten, nichtsdestotrotz auch die Informationspflichten aus Art. 13 u. 14 DSGVO einhalten. Diese wurden in dieser Arbeit nicht gesondert betrachtet, weil sich hierbei keine relevanten Fragen ergeben. Es müssen der betroffenen Person lediglich die geforderten Informationen vor der ersten Erhebung ihrer Wesensdaten bereitgestellt werden.

3. Art. 5 Abs. 1 lit. b DSGVO: Zweckbindung

Eine notwendige Voraussetzung für die Verarbeitung von personenbezogenen Daten ist ein zugrundeliegender Zweck. Laut Art. 5 Abs. 1 lit. b DSGVO

i.V.m. ErwG. 39 S. 7 muss dieser Zweck vor der Verarbeitung bereits festgelegt sowie eindeutig und legitim sein. Eine Verarbeitung von personenbezogenen Daten zu mehreren Zwecken wird nicht ausgeschlossen, solange diese den Maßstäben gerecht werden.[726] Mit der Festlegung auf einen Zweck bindet sich der Verantwortliche an diesen, sodass die Verarbeitung der Daten auf eben diesen Zweck begrenzt ist.[727] Mit dieser Zweckbindung soll verhindert werden, dass personenbezogene Daten, die einmal erhoben wurden, nach Belieben verarbeitet werden dürfen, womit das Recht auf informationelle Selbstbestimmung der Betroffenen immer wieder aufs Neue tangiert werden würde.[728] Die festgelegten Zwecke gelten dabei nicht nur für den Verantwortlichen, sondern auch für alle weiteren Dritten, die die Daten weiterverarbeiten (z.B. Auftragsverarbeiter nach Art. 28 DSGVO).[729]

Das Merkmal der „Eindeutigkeit" fordert, dass der Zweck hinreichend bestimmt festgelegt sein muss.[730] Vage Zwecke wie z.B. „zu Marketingzwecken" oder „zur Verbesserung der Nutzerfreundlichkeit" sind ohne weitere Spezifizierung somit meist unzureichend.[731] Auch ein bloßer Verweis auf eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO wird dem Merkmal der „Eindeutigkeit" nicht gerecht.[732] Allerdings ist auch eine zu detaillierte Beschreibung des Zwecks nicht unbedingt eindeutig, da dadurch die schnelle Informationsgewinnung nicht gewährleistet ist.[733] Notwendig ist vielmehr eine sprachlich präzise Ausformulierung von klar definierten Verarbeitungszwecken,[734] die von anderen, ggf. ähnlichen Zwecken eindeutig abgegrenzt werden können.

Die „Legitimität" stellt darauf ab, dass die Zwecke rechtmäßig sein müssen.[735] Diese Rechtmäßigkeit ergibt sich dabei nicht nur aus einer der Rechtsgrundlagen aus Art. 6 Abs. 1 UAbs. 1 DSGVO, sondern nur durch die ganzheitliche Einhaltung des geltenden Rechts (nicht nur des Datenschutz-

726 *Heberlein* (2018), Art. 5 Rn. 13.
727 *Frenzel* (2021) BDSG, Art. 5 Rn. 27.
728 *Herbst* (2020), Art. 5 Rn. 22.
729 *Frenzel* (2021) BDSG, Art. 5 Rn. 29.
730 *Reimer* (2018), Art. 5 Rn. 21.
731 *Art.-29-Gruppe,* WP 203, 2013, S. 16.
732 *Roßnagel/Nebel/Richter*, ZD 2015, S. 455 (458).
733 *Art.-29-Gruppe,* WP 203, 2013, S. 16.
734 *Pötters* (2018), Art. 5 Rn. 14.
735 *Herbst* (2020), Art. 5 Rn. 37.

rechts).[736] Damit überprüft werden kann, ob ein legitimer Zweck in dem Sinne vorliegt, muss das Merkmal der „Eindeutigkeit" bereits erfüllt sein.[737]

Eine Weiterverarbeitung der Daten, die nicht mit dem Zweck vereinbar ist, wird von Art. 5 Abs. 1 lit b DSGVO ausgeschlossen. „Weiterverarbeitung" ist dabei mit einer nachträglichen Zweckänderung gleichzusetzen.[738] Welche Kriterien bei einer Zweckänderung und bei der Prüfung, ob der neue Zweck mit dem ehemaligen Zweck zu vereinbaren ist, zu berücksichtigen sind, wird durch Art. 6 Abs. 4 DSGVO konkretisiert.[739] Dabei wird gefordert, dass der Verantwortliche unter anderem die Verbindungen zwischen dem ursprünglichen und dem neuen Zweck, den Zusammenhang der Datenverarbeitung, insb. in Bezug auf das Verhältnis zwischen Betroffenen und Verantwortlichen, die Art der personenbezogenen Daten, vor allem, ob Daten i.S.v. Art. 9 (besondere Kategorien von personenbezogenen Daten) und 10 (Daten über strafrechtliche Verurteilungen und Straftaten) DSGVO betroffen sind, die möglichen Folgen für die betroffene Person und das Vorhandensein von geeigneten Garantien (bspw. Verschlüsselung, Pseudonymisierung), berücksichtigt. Die verwendete Formulierung „unter anderem" zeigt allerdings, dass hier keine abschließende Aufzählung vom Gesetzgeber vorgenommen wurde. Somit kann zwar die strikte Zweckbindung aufgehoben, aber nicht frei ein beliebig neuer Zweck festgelegt werden.[740] Ebenso gelten für den neuen Zweck die gleichen Kriterien wie für den ehemaligen Zweck, sodass dieser eindeutig und legitim festgelegt und auch der betroffenen Person gemäß Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO mitgeteilt werden muss.[741] Sollte eine Weiterverarbeitung unzulässig sein, da diese nicht mit dem ehemaligen Zweck vereinbar ist, besteht für den Verantwortlichen nichtsdestotrotz die Möglichkeit, die Daten erneut, unter Berücksichtigung der gesetzlichen Vorschriften, zu erheben, um dabei den neuen Zweck als Verarbeitungsgrundlage festzulegen.[742]

Ergänzend legt Art. 4 Abs. 4 DSGVO aber ebenso fest, wann eine Zweckänderung ohne Berücksichtigung dieser Kriterien möglich ist.[743] Eine solche Ausnahme gilt laut Gesetzestext i.V.m. ErwG. 50 S. 7 dann, wenn die

736 *Art.-29-Gruppe,* WP 203, 2013, S. 19 ff.; *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 8; *Herbst* (2020), Art. 5 Rn. 37; *Heberlein* (2018), Art. 5 Rn. 15.
737 *Roßnagel* (2019), Art. 5 Rn. 79.
738 *Herbst* (2020), Art. 5 Rn. 38 ff.
739 *Schantz* (2020), Art. 5 Rn. 21.
740 *Herbst* (2020), Art. 5 Rn. 43.
741 *Art.-29-Gruppe,* WP 203, 2013, S. 26 f.
742 *Herbst* (2020), Art. 5 Rn. 47.
743 Ebenda, Art. 5 Rn. 46.

betroffene Person ihre Einwilligung zur Zweckänderung gegeben hat oder wenn eine andere Rechtsvorschrift der Union oder der Mitgliedsstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses i.S.v. Art. 23 Abs. 1 DSGVO darstellt, eine solche Zweckänderung verlangt.

Hinzu kommt, dass der Gesetzgeber ebenso Ausnahmen formuliert, bei denen eine Weiterverarbeitung auch ohne Zweckvereinbarkeit möglich ist. Gemäß Art. 5 Abs. 1 lit. b DSGVO sind demnach Archivzwecke, die im öffentlichen Interesse liegen, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke entsprechend privilegiert, unabhängig davon, wer diese Zwecke konkret verfolgt,[744] solange diese den Anforderungen von Art. 89 Abs. 1 DSGVO gerecht werden. Art. 89 Abs. 1 DSGVO fordert, dass bei diesen priorisierten Verarbeitungszwecken geeignete Garantien vorhanden sein müssen, um eine Einhaltung der Verordnung sicherzustellen. Geeignete Garantien sind hierbei nach ErwG. 156 S. 6 vor allem technische und organisatorische Maßnahmen, die die Sicherheit der Verarbeitung sowie u.a. eine maximale Datenminimierung gewährleisten sollen. Dabei ist besonders zu prüfen, ob die betroffenen personenbezogenen Daten nicht auch anonymisiert werden können, ohne, dass die Erreichung des konkreten privilegierten Zwecks verhindert wird.[745] Von Archivzwecken, die im öffentlichen Interesse liegen, spricht man laut ErwG. 158 für gewöhnlich dann, wenn aus den Daten ein bleibender Wert für das allgemeine öffentliche Interesse hervorgeht. Wissenschaftliche Forschungszwecke sollen wiederum gemäß ErwG. 159 ein breites Spektrum an technologischen Entwicklungen, Grundlagenforschungen, angewandte Forschungen und auch privat finanzierten Forschungen abdecken. Ergänzt wird dies durch historische Forschungszwecke, die nach ErwG. 160 auch die Genealogie umfassen, wobei die Tatsache zu berücksichtigen ist, dass die DSGVO nicht für verstorbene Personen gilt. Unter statistischen Zwecken versteht ErwG. 162 die Erhebung und Verarbeitung von personenbezogenen Daten, um mithilfe dieser Daten statistische Auswertungen und Ergebnisse zu erstellen. Zu welchem genauen Zweck diese statistischen Auswertungen und die Erstellung von statistischen Ergebnissen vorgenommen werden dürfen, wird durch die DSGVO nicht abschließend spezifiziert. Damit sind kommerzielle statistische Auswertungen nicht prinzipiell ausgeschlossen.

744 *Reimer* (2018), Art. 5 Rn. 27.
745 *Buchner/Tinnfeld* (2020), Art. 89 Rn. 21.

Allerdings setzt ErwG. 162 S. 5 voraus, dass diese erstellten statistischen Ergebnisse nicht mehr personenbezogene Daten sind, sondern nur noch aggregierte Daten, die keine Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen mehr ermöglichen. Damit werden dann im Umkehrschluss die gängigen kommerziellen statistischen Auswertungen ausgeschlossen, da damit faktisch kein Scoring, Profiling und auch keine anderen derartigen Big-Data Auswertungen vorgenommen werden können.[746]

Diese Ausnahmen der Zweckvereinbarkeit werfen die Frage auf, ob eine vom Primärzweck gesonderte Rechtsgrundlage für die genannten Verarbeitungszwecke vorliegen muss. Um eine unnötige Schwächung der Zweckbindung zu vermeiden, sollte ein restriktiver Umgang gewählt werden.[747] Demnach sollte auch bei einer Zweckänderung, hin zu den privilegierten Verarbeitungszwecken nach Art. 5 Abs. 1 lit. b Hs. 2 DSGVO, die Notwendigkeit einer ausreichenden Rechtsgrundlage gemäß Art. 6 Abs. 1 UAbs. 1 DSGVO bestehen.[748] Es muss allerdings anerkannt werden, dass die DSGVO in dieser Frage einigen Spielraum offenlässt, womit eine Weiterverarbeitung zu den privilegierten Zwecken auch ohne gesonderte Rechtsgrundlage grundsätzlich denkbar und möglich ist.[749]

4. Zweckbindung bei der Verarbeitung von Wesensdaten

Eindeutige und präzise Zwecke zu definieren, sollte beim Einsatz von BCI und der damit einhergehenden Verarbeitung von Wesensdaten kein Problem sein. Denkbar wären bspw. Zwecke wie „Steuerung von Peripheriegeräten im Smart Home", „Passive Auswertung der Gehirnaktivitäten, um Feedback bzgl. Aufmerksamkeit, psychischer Gesundheit und Schlafqualität zu geben" oder „Neurologisch gesteuertes Gaming".

Interessanter ist allerdings die Zweckänderung. Die Kriterien nach Art. 6 Abs. 4 DSGVO, die bei einer Zweckänderung maßgeblich sind, werden bei der Verarbeitung von Wesensdaten kaum eine Weiterverarbeitung rechtfertigen können. Dies ist durch den grundsätzlichen Aussagegehalt von Wesensdaten begründet, womit die möglichen Folgen für die betroffene

746 *Richter*, DuD 2015, S. 735 (738 f.); *Culik/Döpke,* ZD 2017, S. 226 (230); *Schantz* (2016) Art. 89 Rn. 24 f.
747 *Voigt* (2019), Art. 5 Rn. 26.
748 *Herbst* (2020), Art. 5 Rn. 54.
749 *Roßnagel* (2019), Art. 5 Rn. 109.

Person ein Ausschlusskriterium sein dürften, auch wenn eine grundsätzliche Vereinbarkeit zum ehemaligen Zweck vorliegt.

Eine Weiterverarbeitung auf Grundlage von Art. 5 Abs. 1 lit. b DSGVO, bei der also die Zweckvereinbarung nicht mehr notwendig ist, ist wiederum oftmals denkbar. Archivzwecke, die einen bleibenden Wert für das öffentliche Interesse haben, und historische Forschungszwecke dürften bei der Datenverarbeitung durch BCI ausgeschlossen sein. Unter Berücksichtigung ausreichender technischer und organisatorischer Maßnahmen ist eine Weiterverarbeitung zu wissenschaftlichen Forschungszwecken und statistischen Zwecken allerdings durchaus denkbar. Die KI-Forschung und das damit einhergehende Training von bspw. Large-Language-Models könnten als ein solcher wissenschaftlicher Forschungszweck definiert werden. Gleiches gilt auch für die Gehirnforschung und die damit einhergehende Identifikation von bestimmten neurologischen Abläufen. Statistische Zwecke könnten wiederum interne Auswertungen sein, um nachvollziehen zu können, welche Tätigkeiten bevorzugt mit BCI ausgeführt werden.

5. Art. 5 Abs. 1 lit. c DSGVO: Datenminimierung

In der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO findet sich ein weiterer Grundsatz der Datenverarbeitung. Dieser fordert, dass bei einer Verarbeitung von personenbezogenen Daten, diese Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Mit der Ausrichtung der Datenminimierung am Zweck der Verarbeitung findet eine Verknüpfung mit der Zweckbindung aus Art. 5 Abs. 1 lit. b DSGVO statt, die erneut die Notwendigkeit von festgelegten und legitimen Zwecken unterstreicht und den Zweck als zentralen Orientierungspunkt etabliert.[750]

Dem Zweck angemessen sind Daten dann, wenn sie einen hinreichenden sachlichen Bezug zur Funktion, zum Inhalt und zum Umfang des Verarbeitungszwecks haben.[751] Die Bewertung, ob eine Angemessenheit vorliegt, sollte dabei objektiv und mit einer gewissen Distanz vorgenommen werden.[752] Zentral steht dabei die Frage, ob die personenbezogenen Daten

750 *Herbst* (2020), Art. 5 Rn. 56.
751 *Roßnagel* (2019), Art. 5 Rn. 119.
752 *Frenzel* (2021) BDSG, Art. 5 Rn. 35.

einen angemessen Bezug zum Zweck haben und überhaupt geeignet sind, um den Verarbeitungszweck zu erreichen.[753]

Das Merkmal der Erheblichkeit erfordert wiederum, dass die Daten einen zielführenden Unterschied bei der Zweckerfüllung bewirken und eine notwendige Bedeutung für den Zweck haben.[754] Auch dieser Bestandteil ist objektiv zu bewerten und nicht von den Bedürfnissen des Verantwortlichen abhängig zu machen.[755]

Mit der Begrenzung der Daten auf das notwendige Maß, legt der Gesetzgeber fest, dass nur solche personenbezogenen Daten verarbeitet werden dürfen, ohne welche eine Erreichung des Verarbeitungszwecks unmöglich wäre.[756] Die Menge der Daten ist demnach immer dann auf das unvermeidbar Erforderliche zu begrenzen, wenn diese für die Erreichung des Zwecks nicht essenziell sind.[757] Dabei spielt es auch keine Rolle, ob die Daten angemessen und/oder erheblich sind.[758]

Übergeordnetes Ziel der Datenminimierung ist es somit, die Anzahl der verarbeiteten personenbezogenen Daten sowie die Anzahl der Verarbeitung dieser Daten zu minimieren[759] und diese Minimierung auch zukünftig zu optimieren.[760] Ebenso sollen damit überbordende Parallelspeicherungen von identischen personenbezogenen Daten teilweise verhindert[761] und eine Anonymisierung von Daten begünstigt und gefördert werden, da diese wirksam den Personenbezug der Daten minimiert.[762]

6. Datenminimierung bei der Verarbeitung von Wesensdaten

Ohne die Verarbeitung von Wesensdaten würde ein BCI nicht funktionstüchtig sein. Damit sind Wesensdaten grundsätzlich sowohl angemessen sowie erheblich für den Verarbeitungszweck. Relevant ist somit vor allem die Begrenzung der Daten auf das notwendige Maß. Dies ist besonders darum eine Herausforderung, da BCI ständig die Gehirnaktivitäten auf-

753 *Herbst* (2020), Art. 5 Rn. 57; *Roßnagel* (2019), Art. 5 Rn. 119.
754 *Roßnagel* (2019), Art. 5 Rn. 120.
755 *Frenzel* (2021) BDSG, Art. 5 Rn. 36.
756 *Roßnagel* (2019), Art. 5 Rn. 121.
757 *Herbst* (2020), Art. 5 Rn. 57; *Roßnagel* (2019), Art. 5 Rn. 125.
758 *Roßnagel* (2019), Art. 5 Rn. 121.
759 *Gola* (2018), Art. 5 Rn. 22.
760 *Roßnagel* (2019), Art. 5 Rn. 127.
761 *Voigt* (2019), Art. 5 Rn. 28.
762 *Herbst* (2020), Art. 5 Rn. 58; *Roßnagel* (2019), Art. 5 Rn. 125.

zeichnen, damit die relevanten Signale erkannt werden können. Allerdings wird es oftmals so sein, dass nur ein Bruchteil aller Gehirnaktivitäten tatsächlich relevant sind. Demnach werden etliche neurologische Aktivitäten verarbeitet, die nicht notwendig sind. Die Vorschläge aus Kapitel I.VI.2 könnten hier Abhilfe schaffen, indem das Gerät nur auf Befehl des Nutzers aktiv wird und Gehirnaktivitäten aufzeichnet sowie lediglich zielgerichtet Signale aus relevanten Gehirnregionen aufzeichnet und diese dann noch automatisiert vorfiltert.

7. Art. 5 Abs. 1 lit. d DSGVO: Richtigkeit

Bereits das BVerfG hatte in seinem wegweisenden Volkszählungsurteil aus dem Jahre 1983 darauf hingewiesen, dass durch die digitale Datenverarbeitung umfassende Persönlichkeitsprofile erstellt werden können, über die betroffene Personen keinerlei Kontrolle bzgl. Richtigkeit und Verwendung der Daten mehr haben.[763] Im gleichen Verständnis fordert Art. 5 Abs. 1 lit. d DSGVO, dass personenbezogene Daten sachlich richtig sowie erforderlichenfalls auf dem neuesten Stand sein müssen und, dass angemessene Maßnahmen ergriffen werden müssen, um personenbezogene Daten, die in Bezug auf den zugrundeliegenden Zweck unrichtig sind, unverzüglich zu löschen oder zu berichtigen.

Sachlich richtig sind personenbezogene Daten dann, wenn diese nach objektiver Einschätzung der Realität entsprechen.[764] Nur so kann gewährleistet werden, dass Sachverhalte und Situationen, die die betroffene Person betreffen, wahrheitsgemäß auf Grundlage der Daten rekonstruiert werden können.[765] Diese Voraussetzung betrifft dabei nicht nur Tatsachenangaben, sondern auch Werteurteile, wenn diese bspw. auf falschen Tatsachen beruhen oder von falschen Prämissen ausgehen.[766]

Während die sachliche Richtigkeit grundsätzlich zu beachten ist, müssen personenbezogene Daten lediglich „erforderlichenfalls" auf dem neusten Stand sein.[767] Wenn der Verarbeitungszweck eine Verarbeitung von historischen Daten notwendig macht, z.B. wenn in einer Patientenakte noch Ge-

763 BVerfG, Urt. v. 15.12.1983 - 1 BvR 209/83, NJW 1984, 421.
764 *Herbst* (2020), Art. 5 Rn. 60.
765 *Frenzel* (2021) BDSG, Art. 5 Rn. 39.
766 *Schantz* (2020), Art. 5 Rn. 27; anderer Meinung: *Herbst* (2020), Art. 5 Rn. 60; *Roßnagel* (2019), Art. 5 Rn. 140.
767 *Voigt* (2019), Art. 5 Rn. 31.

sundheitszustände festgehalten sind, die zwar zum jetzigen Zeitpunkt nicht mehr die Realität abbilden, aber eine Entwicklung dokumentieren, dann müssen die Daten nicht nur dem neusten Stand angepasst werden.[768] Ob eine Anpassung der Daten an dem neusten Stand tatsächlich erforderlich ist, ist daran zu bemessen, inwiefern unrichtige Daten schädlich für den Verarbeitungszweck und damit auch für die betroffenen Personen sind.[769] Dies trifft meistens dann zu, wenn die Aktualität der personenbezogenen Daten wesentlich für den Verarbeitungszweck ist. So ist es bspw. bei der Prüfung einer möglichen Kreditvergabe zwingend notwendig, dass Daten zum Vermögen, zum Einkommen und zu bestehenden Schulden auf dem neusten Stand sind, damit eine faire Kreditvergabe vorgenommen werden kann.

Art. 5 Abs. 1 lit. d Hs. 2 DSGVO ergänzt diese Kriterien um die Notwendigkeit, unrichtige Daten unverzüglich zu berichtigen oder zu löschen. Daraus geht hervor, dass der Verantwortliche angemessene Maßnahmen ergreifen muss, um die Richtigkeit der personenbezogenen Daten kontinuierlich und aktiv zu überprüfen.[770] Eine solche Maßnahme könnte kontextbedingt z.B. eine regelmäßige Kontrolle des Datenbestands[771] bzw. dessen Abgleich mit Angaben der betroffenen Personen sein. Erweitert wird dieses Merkmal um das Recht der betroffenen Person auf Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) und Einschränkung der Verarbeitung (Art. 18 DSGVO).

Die Richtigkeit der Daten spielt besonders dann eine Rolle, wenn die betroffene Person auf Grundlage der personenbezogenen Daten Rechtsfolgen zu befürchten hat.[772] In diesem Zuge sind vor allem Profiling-Maßnahmen erwähnenswert, die ggf. große Auswirkungen für die Rechte und Freiheiten der betroffenen Person haben könnten.[773] Aus diesem Grund konkretisiert ErwG. 71 S. 6 auch, dass beim Profiling geeignete technische und organisatorische Maßnahmen getroffen werden müssen, die ausreichend sicherstellen, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird. Auch bei KI ist dahingehend zu berücksichtigen, dass geeignete Trainings-

768 *Roßnagel* (2019), Art. 5 Rn. 141; *Herbst* (2020), Art. 5 Rn. 61; *Voigt* (2019), Art. 5 Rn. 31.
769 *Reimer* (2018), Art. 5 Rn. 36; *Herbst* (2020), Art. 5 Rn. 62.
770 *Pötters* (2018), Art. 5 Rn. 24.
771 *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 13.
772 *Frenzel* (2021) BDSG, Art. 5 Rn. 39.
773 *Art.-29-Gruppe,* WP 251 1 rev. 01, 2017, S. 11.

daten verwendet werden, damit die KI nicht falsche oder diskriminierende Ergebnisse/Daten erzeugt.[774]

8. Richtigkeit bei der Verarbeitung von Wesensdaten

Im Zuge der Betrachtung der Einwilligung mittels BCI wurde bereits festgestellt, dass die Übersetzung der Gehirnaktivitäten in entsprechende Outputs ein Problem darstellen könnten, wenn diese nicht korrekt ist. Dieser Aspekt ist auch bei der Einhaltung des Grundsatzes der Richtigkeit relevant. Verantwortliche müssen demnach sicherstellen, dass die relevanten Signale korrekt aufgezeichnet werden sowie, dass die zugrundeliegende Software lediglich richtige Urteile trifft, die den zugrundeliegenden Signalen entsprechen.

Diese Maßgabe überträgt sich auch auf die notwendige Aktualität der Daten. Während die neurologischen Signale logischerweise zu jeder Zeit aktuell sind, da diese in Echtzeit direkt aus dem Gehirn der Nutzer ausgelesen werden, muss dies für die Übersetzung nicht gelten. Es ist bspw. denkbar, dass neue Erkenntnisse zu Gehirnaktivitäten dazu führen, dass auch die Übersetzung angepasst werden muss. Der Verantwortliche muss demnach kontinuierlich sicherstellen, dass die eingesetzten Systeme neue Informationen berücksichtigen, damit die Übersetzung zu jeder Zeit aktuell ist. Insbesondere bedeutet dies, dass die Richtigkeit bei den Trainingsdaten des Übersetzungsalgorithmus gewährleistet werden muss. Diese kontinuierliche Überprüfung würde ebenso sicherstellen, dass keine unrichtigen Daten mehr verarbeitet werden würden.

9. Art. 5 Abs. 1 lit. e DSGVO: Speicherbegrenzung

Um eine zeitlich unbegrenzte Speicherung von personenbezogenen Daten zu verhindern, fordert die DSGVO, dass die Möglichkeit der Identifizierung einer betroffenen Person nur so lange durch die Daten ermöglicht werden darf, wie es für den zugrundeliegenden Zweck notwendig ist. Damit ergänzt der Gesetzgeber die Zweckbindung um eine zeitliche Komponente.[775] Durch ErwG. 39 S. 8 wird konkretisiert, dass sich die Speicherfrist

774 *Schantz* (2020), Art. 5 Rn. 27.
775 *Pötters* (2018), Art. 5 Rn. 25; *Herbst* (2020), Art. 5 Rn. 65.

an dem unbedingt erforderlichen zeitlichen Mindestmaß zu orientieren hat. Der Begriff „Speichern" beschreibt dabei das technische Vorhalten von Daten, um diese weiter zu verarbeiten oder zu nutzen.[776]

Dabei gibt es verschiedene Möglichkeiten, dieser Verpflichtung der Speicherbegrenzung nachzukommen. Naheliegend ist die Löschung der Daten vom entsprechenden Datenträger, sodass diese nicht mehr aufrufbar sind und somit auch keine Identifikation von Betroffenen mehr möglich ist.[777] Gleiches kann auch erreicht werden, wenn die relevanten Datenträger ausreichend zerstört werden.[778] Abschließend geht aus der konkreten Formulierung des Gesetzestexts noch eine andere Möglichkeit hervor. Art. 5 Abs. 1 lit. e DSGVO stellt nämlich nicht auf die Speicherung als solche ab, sondern auf die Möglichkeit der Identifizierung der betroffenen Person.[779] Demnach ist eine Speicherbegrenzung auch mit einer Anonymisierung der personenbezogenen Daten denkabr, womit die Identifikation der Betroffenen nicht mehr möglich wäre.[780]

Damit Verantwortliche sich auch tatsächlich an diese Vorgaben halten, sieht ErwG. 39 S. 10 vor, dass dieser Fristen für die Löschung oder die regelmäßige dahingehende Überprüfung von personenbezogenen Daten festlegt. Sinnvoller ist es allerdings, die Fristsetzung nicht alternativ zur Überprüfung zu sehen und vice versa, sondern diese Maßnahmen als gegenseitige Ergänzung zu verstehen.[781] Ein Verantwortlicher muss somit genau wissen, welche Datenarten verarbeitet werden und welche gesetzlichen Aufbewahrungs- und Löschpflichten bestehen, damit diese mit den eigenen Aufbewahrungsinteressen abgeglichen werden können, um dann konkrete Aufbewahrungs- und Löschfristen für die jeweiligen Datenarten festzulegen, anhand derer eine kontrollierte Löschung garantiert werden kann.[782] Dieser Prozess sollte zusätzlich regelmäßig auf Aktualität und Angemessenheit überprüft werden.

Wie bei der Zweckbindung gemäß Art. Art. Abs. 1 lit. b DSGVO besteht eine Ausnahme von der Speicherbegrenzung, wenn personenbezogene Daten ausschließlich für im öffentlichen Interesse liegende Archivzwecke, für

776 *Roßnagel* (2019), Art. 4 Rn. 19.
777 *Herbst* (2020), Art. 5 Rn. 66.
778 *Reimer* (2018), Art. 5 Rn. 40.
779 *Roßnagel* (2019), Art. 5 Rn. 155.
780 *Herbst* (2020), Art. 5 Rn. 66; *Roßnagel* (2019), Art. 5 Rn. 155; *Reimer* (2018), Art. 5 Rn. 40.
781 *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 14.
782 *Voigt* (2019), Art. 5 Rn. 36.

wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 DSGVO verarbeitet werden.

10. Speicherbegrenzung bei Verarbeitung von Wesensdaten

Mit der Notwendigkeit der Speicherbegrenzung entsteht ein Spannungsverhältnis beim Einsatz von BCI. Grundsätzlich würde sich die Speicherdauer der verarbeiteten Wesensdaten nach Art. 17 Abs. 1 DSGVO richten, womit die Daten dann gelöscht werden müssten, sobald der Zweck der Verarbeitung erreicht wurde. Bei einer strengen Auslegung würde dies bedeuten, dass die neurologischen Signale und die darauf aufbauenden Übersetzungen dann gelöscht werden müssen, sobald der gewünschte Output erzeugt wurde. Bei einer etwas gemäßigteren Auslegung könnten die Daten noch für eine gewisse Dauer vorgehalten werden, z.B. für einen Monat oder bis die Person die Technologie nicht mehr nutzt oder ihre Einwilligung zurückzieht. Wie allerdings bei der Betrachtung der Richtigkeit der Daten festgestellt wurde, ist der Verantwortliche auch dazu verpflichtet, die Trainingsdaten und die daraus resultierenden Übersetzungen aktuell und korrekt zu halten. Dieser Pflicht kann nur nachgekommen werden, wenn die Daten langfristig gespeichert werden dürfen. Diesem Spannungsverhältnis kann der Verantwortliche allerdings damit entkommen, indem dieser bereits vor Beginn der Verarbeitung bspw. die Einwilligung für den Zweck einholt, dass die erhobenen Wesensdaten auch für die notwendige Optimierung des Systems verwendet werden dürfen. Eine andere Möglichkeit wäre eine Weiterverarbeitung auf Grundlage von Art. 5 Abs. 1 lit. b DSGVO. Das Training des Systems kann als KI-Forschung angesehen werden, womit ein wissenschaftlicher Forschungszweck vorliegen würde.

11. Art. 5 Abs. 1 lit. f DSGVO: Integrität und Vertraulichkeit

Gemäß dem Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. f DSGVO, muss bei der Datenverarbeitung ein angemessener Schutz der personenbezogenen Daten vorliegen. Dieser Schutz soll durch geeignete technische und organisatorische Maßnahmen gewährleistet werden und einschließlich vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung schützen. Die Aufzählung ist dabei nicht abschließend,

sondern nur exemplarisch[783] und macht deutlich, dass eine umfassende IT-Sicherheit gefordert wird.[784] Der Teilaspekt der unbefugten Verarbeitung adressiert dabei vor allem den Zugang zu sowie die Verarbeitung von personenbezogenen Daten durch unbefugte Dritte und der Teilaspekt der unrechtmäßigen Verarbeitung umfasst den Fall, wenn personenbezogene Daten vom Verantwortlichen ohne ausreichende Rechtsgrundlage verarbeitet werden.[785] Auch ErwG. 39 S. 12 stellt nochmal besonders auf die Sicherheit und Vertraulichkeit ab und unterstreicht die Tatsache, dass Unbefugte keinen Zugang zu Daten haben und diese auch nicht verarbeiten sollten. Die Teilaspekte des unbeabsichtigten Verlustes, der unbeabsichtigten Zerstörung und der unbeabsichtigten Schädigung beziehen sich wiederum auf Ereignisse, die vom Verantwortlichen nicht gewollt sind bzw. ohne Absicht stattfinden.[786] Der Verlust stellt dabei Fälle dar, in denen Daten(träger) verloren gehen oder gelöscht werden und eine Zerstörung liegt bspw. vor, wenn Datenträger vernichtet werden oder eine wesentliche Veränderung der Daten stattfindet.[787] Die unbeabsichtigte Schädigung ist ergänzend dazu als umfassende Auffangklausel zu sehen.[788]

12. Integrität und Vertraulichkeit bei der Verarbeitung von Wesensdaten

Um die Risiken einzudämmen, verlangt Art. 5 Abs. 1 lit. f DSGVO geeignete technische und organisatorische Maßnahmen. Diese werden gesetzlich in Art. 32 DSGVO konkretisiert. Im Zuge der Verarbeitung von Wesensdaten sind hier etliche Maßnahmen denkbar. Diese wurden detailliert bereits in Kapitel I.IV betrachtet.

13. Art. 5 Abs. 2 DSGVO: Rechenschaftspflicht

Art. 5 Abs. 2 DSGVO verpflichtet den Verantwortlichen dazu, die Grundsätze aus Abs. 1 einzuhalten. Diese Pflicht gliedert sich in zwei Bestandteile. Erstens muss der Verantwortliche dafür sorgen, dass die Grundsätze der

783 *Frenzel* (2021) BDSG, Art. 5 Rn. 46.
784 *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 15.
785 *Herbst* (2020), Art. 5 Rn. 74.
786 *Reimer* (2018), Art. 5 Rn. 51.
787 *Herbst* (2020), Art. 5 Rn. 75; *Reimer* (2018), Art. 5 Rn. 51.
788 *Reimer* (2018), Art. 5 Rn. 51.

Datenverarbeitung initial umgesetzt sowie fortführend eingehalten werden, und zweitens muss die Umsetzung ergänzend dokumentiert werden, damit diese auch nachgewiesen werden kann.[789] Art. 5 Abs. 2 DSGVO zwingt den Verantwortlichen demnach dazu, ein ganzheitliches Datenschutz-Managementsystem zu implementieren und dessen Status zu überwachen.[790]

Dieses Datenschutz-Managementsystem muss dabei so ausgestaltet sein, dass sich damit die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DSGVO nachweisen lassen. Dies ist besonders unter dem Gesichtspunkt des Art. 58 Abs. 1 lit. a DSGVO relevant, der Aufsichtsbehörden die Befugnis gibt, vom Verantwortlichen alle notwendigen Informationen zu erhalten.[791] Ergänzend dazu greift diese Nachweispflicht des Verantwortlichen auch in konkreten Streitfällen und führt hier zu einer Beweislastumkehr zu Gunsten von betroffenen Personen.[792] Da es für betroffenen Personen nur selten möglich ist, eindeutig zu beweisen, dass eine rechtswidrige Verarbeitung ihrer Daten vorliegt, ist es demnach die Pflicht des Verantwortlichen, darzulegen, dass seine Datenverarbeitung rechtmäßig ist.

Eine Konkretisierung der notwendigerweise zu ergreifenden Nachweismittel findet an vielen verschiedenen Stellen in der DSGVO statt. Besonders erwähnenswert sind dabei vor allem Art. 24 (technische und organisatorische Maßnahmen), Art. 28 Abs. 3 (Auftragsverarbeitungsverträge), Art. 30 (Verarbeitungsverzeichnis), Art. 33 f. (Meldung von Datenpannen) und Art. 35 DSGVO (Datenschutz-Folgenabschätzung).[793] Wie lange diese Nachweismittel vorgehalten und aufbewahrt werden müssen, wird allerdings nicht konkretisiert.[794] Eine dauerhafte Aufbewahrung ist demnach naheliegend, widerspricht allerdings dem risikobasierten Ansatz der DSGVO.[795] Auch formell macht die DSGVO keine Vorgaben dazu, wie die Nachweismittel vorgehalten werden müssen, wobei rein logisch eine schriftliche Dokumentation zu empfehlen ist.[796]

Sollte ein Verantwortlicher seiner Rechenschaftspflicht nicht nachkommen und die Einhaltung der Grundsätze nicht nachweisen können, könn-

789 *Roßnagel* (2019), Art. 5 Rn. 174.
790 *Frenzel* (2021) BDSG, Art. 5 Rn. 52.
791 *Herbst* (2020), Art. 5 Rn. 79.
792 *Pötters* (2018), Art. 5 Rn. 34.
793 Ein detaillierter Vorschlag zu den notwendigen Nachweismitteln: *Voigt* (2019), Art. 5 Rn. 41 ff.
794 *Herbst* (2020), Art. 5 Rn. 80; *Voigt* (2019), Art. 5 Rn. 44.
795 *Voigt* (2019), Art. 5 Rn. 44 - leitet darum einen dreijährige Aufbewahrungsfrist aus dem Ordnungswidrigkeitengesetz ab (OWiG).
796 *Herbst* (2020), Art. 5 Rn. 80; *Voigt* (2019), Art. 5 Rn. 45.

te dies gemäß Art. 83 Abs. 5 lit. a DSGVO mit einem Bußgeld von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs bestraft werden. Eine Haftungsbefreiung gemäß Art. 82 Abs. 3 DSGVO ist ohne Einhaltung der Rechenschaftspflicht ebenso ausgeschlossen.[797]

14. Rechenschaftspflicht bei der Verarbeitung von Wesensdaten

In dieser Arbeit wurde detailliert auf die technischen und organisatorischen Maßnahmen sowie auf die Datenschutz-Folgenabschätzung eingegangen. Dabei wurde gezeigt, welche Maßnahmen ergriffen werden können und wie eine Dokumentation zur Datenschutz-Folgenabschätzung aussehen sollte.

Auf Auftragsverarbeitungsverträge, Verarbeitungsverzeichnis und die Meldung von Datenpannen wurde nicht gesondert eingegangen. Grund dafür ist, dass diese Pflichten keine Besonderheit bei der Verarbeitung von Wesensdaten mittels BCI mit sich bringen und somit nicht relevant für die Beantwortung der Forschungsfrage sind. Demnach gilt auch für Verantwortliche, die Wesensdaten verarbeiten, dass diese entsprechende Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO dokumentieren, Datenpannen nach Art. 33 u. 34 DSGVO melden müssen sowie dafür verantwortlich sind, dass Auftragsverarbeitungsverträge i.S.v. Art. 28 Abs. 3 DSGVO abgeschlossen werden, sobald Dritte mit der Verarbeitung von Wesensdaten beauftragt werden.

797 *Herbst* (2020), Art. 5 Rn. 79.

L. Zwischenfazit

Die durchgeführte Analyse der wichtigsten DSGVO-Vorgaben und die Anwendung der daraus resultierenden Erkenntnisse auf den speziellen Fall von BCI und der damit einhergehenden Verarbeitung von Wesensdaten, sollte aufzeigen, ob die derzeitigen Vorgaben in Zukunft ausreichend sein werden, um die neuartige Technologie datenschutzrechtlich zu regulieren.

1. Anwendungsbereich

Im Zuge der Erarbeitung wurde festgestellt, dass die Verarbeitung von Wesensdaten durch BCI in den sachlichen Anwendungsbereich der DSGVO fällt. Wesensdaten sind demnach effektiv als personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO zu definieren. Fraglich ist allerdings, ob diese Daten auch allgemein unter den besonderen Schutz des Art. 9 DSGVO fallen und als besondere Kategorien von personenbezogenen Daten definiert werden können. Es wurde festgestellt, dass die diesbezügliche Einstufung von Wesensdaten, je nach Herangehensweise, unterschiedlich ausfällt. Bei einer kontextabhängigen Bewertung dürften Wesensdaten für gewöhnlich als besondere Kategorien von personenbezogenen Daten gelten, bei der zweckabhängigen Einstufung hingegen, ist eine solche allgemeine Einordnung in den Reglungsbereich von Art. 9 DSGVO nicht gegeben. Besonders mit Blick auf die bereits gängige Praxis bei der Bewertung von personenbezogenen Daten und deren Sensitivität, ist zu erwarten, dass Wesensdaten nicht generell von Verantwortlichen als besondere Kategorien von personenbezogenen Daten eingestuft werden dürften.

2. Rechtsgrundlagen

Fortfolgend wurde festgestellt, dass die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO in Zukunft als legitime Rechtsgrundlage für die Verarbeitung von Wesensdaten herangezogen werden kann. Allerdings wurde ebenso festgestellt, dass eine Einwilligung in der momentanen Anwendung häufig nicht die rechtlichen Vorgaben gemäß Informiertheit und Freiwilligkeit einhält. Dies wurde als zukünftiges Risiko bei der Verarbeitung von Wesens-

daten identifiziert. Ergänzend wurde dargelegt, dass wirksame Einwilligungen in Zukunft theoretisch auch per neurologischem Signal und mithilfe von BCI gegeben werden können. Herausforderung dabei ist lediglich die Gewährleistung der allgemeinen Eindeutigkeit bei der Übersetzung von Hirnströmen in Handlungen.

Neben der Einwilligung wurde auch das berechtigte Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO als mögliche Rechtsgrundlage bei der Verarbeitung von Wesensdaten identifiziert. Mithilfe einer beispielhaften Interessenabwägung wurde gezeigt, wie eine solche Legitimation in Zukunft aussehen könnte. Diese kommt allerdings nur in Betracht, da Wesensdaten nicht kategorisch unter Art. 9 Abs. 1 DSGVO fallen. Damit würde ein Risiko für betroffene Personen entstehen.

3. Betroffenenrechte: Auskunftsrecht

Die gesetzlichen Vorgaben zum Auskunftsrecht wurden wiederum als ausreichend identifiziert. Die Aufbereitung der Daten kann in einer Weise gewährleistet werden, die die Verständlichkeit für die betroffene Person erhöht, ohne die Aussagekraft oder den Umfang der Datenkopie zu beschränken. Herausforderung dabei ist lediglich die Entfernung von Daten Dritter. Hierbei würde eine Interessenabwägung allerdings bereits ein zufriedenstellendes Ergebnis liefern. Dabei kann sichergestellt werden, dass der Eingriff in die Privatsphäre der dritten Person so gering wie möglich bleibt, sodass das Auskunftsrecht nicht unnötig beschränkt werden muss.

Ebenso ist es möglich, der betroffenen Person verständlich und ausreichend mitzuteilen, wie sich die automatisierte Entscheidungsfindung gestaltet. Ob eine solche Mitteilung notwendig ist, ist abhängig vom konkreten Einsatz des BCI. Bei anlassbezogenen Verarbeitungen, die nur aufgrund eines menschlichen Inputs/eines neurologischen Befehls stattfinden, ist im Normalfall nicht von automatisierter Entscheidungsfindung auszugehen.

4. Technischer Datenschutz

Die Regularien zum technischen Datenschutz wurden ebenso als ausreichend wahrgenommen. Der in der DSGVO gesetzte Rahmen bietet genug Spielraum und Orientierung, um eine technische Sicherheit von Wesensdaten zu garantieren. Problematisch in diesem Zusammenhang ist allerdings,

dass diese Reglungen nur für die Verantwortlichen der Datenverarbeitung gelten. Hersteller sind nicht dazu verpflichtet z.B. die Vorgaben zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen umzusetzen. Dies könnte in Zukunft ein Risiko für BCI-Nutzer darstellen, da es Verantwortlichen dadurch erschwert werden könnte, die Pflichten einzuhalten.

5. Organisatorischer Datenschutz

Auch wurde die DSFA als Kernstück des organisatorischen Datenschutzes betrachtet. Die Prüfung hat ergeben, dass bei einer Verarbeitung von Wesensdaten mithilfe von BCI regelmäßig eine DSFA notwendig sein wird. Anhand eines beispielhaften Falles wurde eine entsprechende DSFA durchgeführt, um aufzuzeigen, wie eine solche zukünftig gestaltet werden könnte.

6. Grundlagen der Verarbeitung

Als letzter Punkt der vorgelagerten Analyse wurden die Grundsätze der Verarbeitung aus Art. 5 DSGVO auf die Verarbeitung von Wesensdaten angewendet. Dabei wurde festgestellt, dass alle Grundsätze eingehalten werden können.

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.).

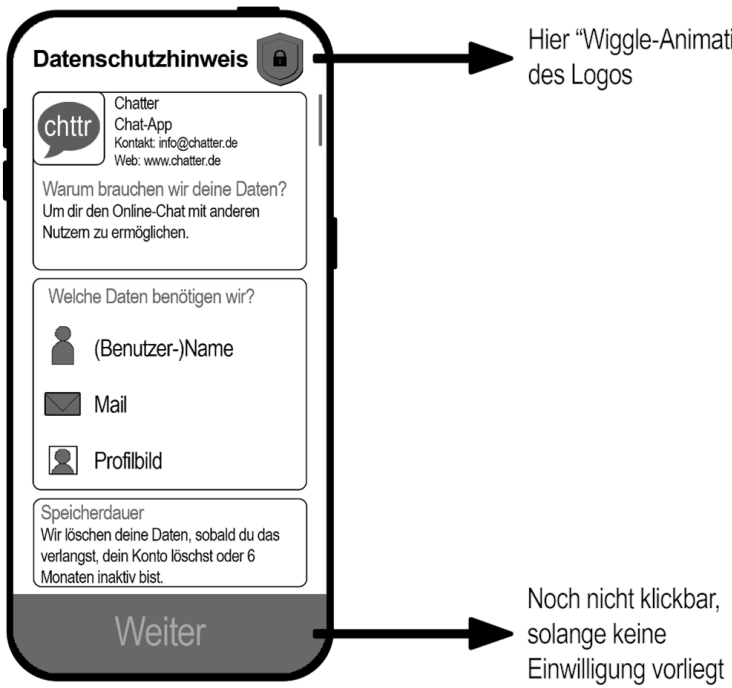
817 *Gluck et al.,* Proceedings of the Twelfth Symposium on Usable Privacy and Security 2016, S. 321 (323 ff.).

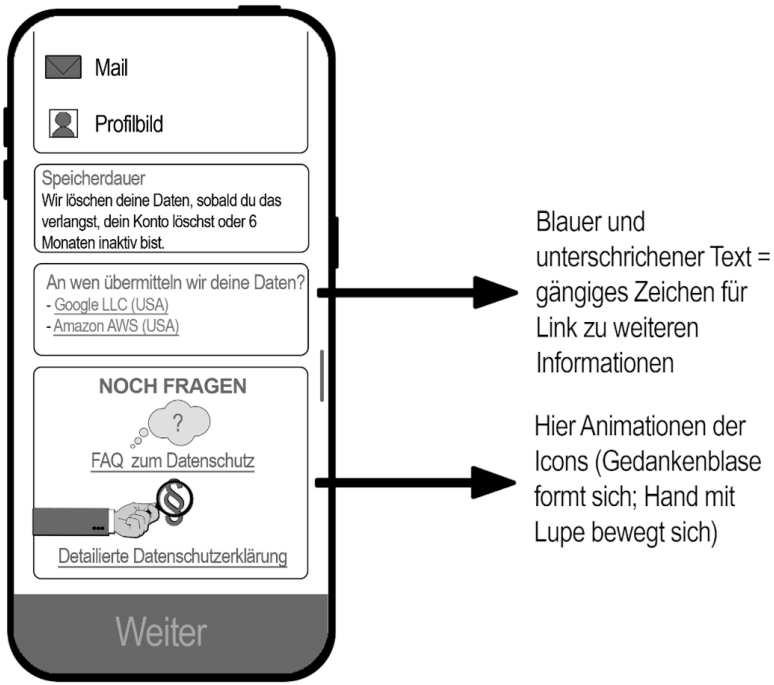
Information über die Datenverarbeitung meist nicht mit einer deutlich kürzeren Form vereinbar ist, bietet es sich an, dass der betroffenen Person standardgemäß nur die wichtigsten, für die Entscheidung relevanten Informationen als prägnante Aufzählung präsentiert werden. Die wichtigen, für die Entscheidung 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]

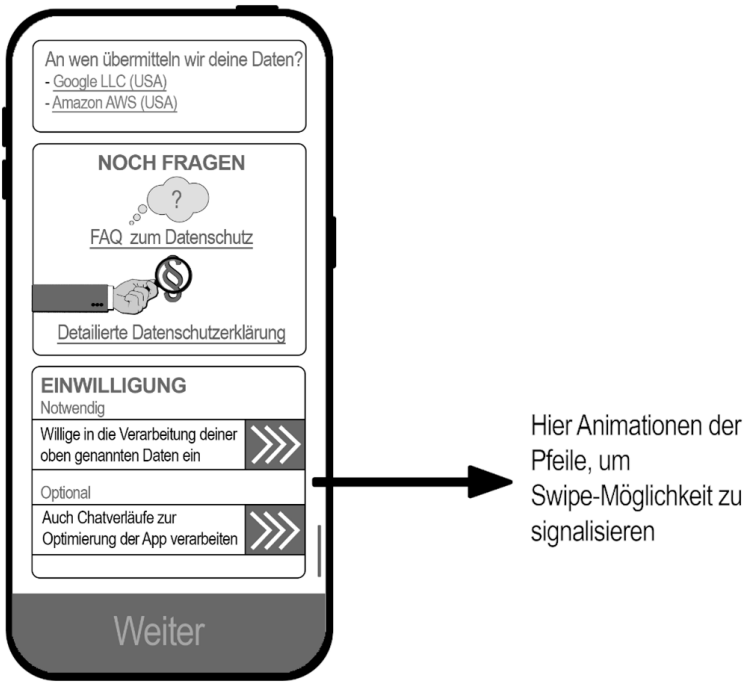
Aus der Auswertung der relevanten wissenschaftlichen Literatur geht demnach hervor, dass für eine informierte Einwilligung drei Aspekte notwendig sind: 1. Aufmerksamkeit/Interesse, 2. prägnante und verständliche Informationsvermittlung und 3. einfache und zielführende Interaktion. Unter Berücksichtigung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

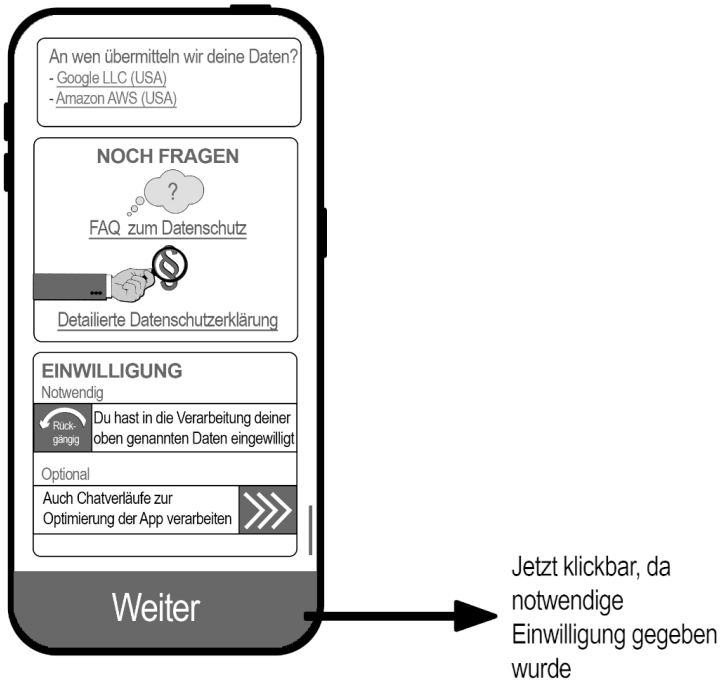
818 *Bergram et al.,* ECIS 2020 Research Papers 2020, S. 1 (1 ff.).
819 *Lindegren et al.,* Behaviour & Information Technology 2019, S. 398 (406 ff.).

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.

N. Abschluss und Anfang

1. Erkenntnisse der Arbeit

Diese Arbeit hat es sich zur Aufgabe gemacht, zu überprüfen, ob das bestehende europäische Datenschutzrecht ausreichend ist, um die zukünftige Datenverarbeitung mittels BCI ausreichend und sinnvoll zu regulieren.

Dabei wurde festgestellt, dass die Daten, die durch Neurotechnologie verarbeitet werden, als personenbezogene Daten zu definieren sind. Diese Daten können aufgrund ihres außergewöhnlichen Aussagegehalts als Wesensdaten bezeichnet werden. Fraglich ist allerdings, ob diese Wesensdaten allgemeinhin auch zu den besonderen Kategorien von personenbezogenen Daten gezählt werden können. Ausgehend von der bisherigen Praxis wurde festgestellt, dass diese in Zukunft nicht den besonderen Schutz des Art. 9 DSGVO genießen dürften. Dies könnte ein Problem darstellen.

Anschließend wurden einschlägige Rechtsgrundlagen betrachtet. Der Fokus lag dabei auf der Einwilligung sowie auf dem berechtigten Interesse. Es wurde festgestellt, dass die Einwilligung zwar eine legitime Rechtsgrundlage sein kann, aber grundsätzlich die Frage besteht, ob derzeit die Anforderungen an Informiertheit und Freiwilligkeit überhaupt erfüllt werden können. Dies wurde ebenso als mögliches Problem bei der Verarbeitung von Wesensdaten identifiziert.

Neben der Einwilligung wurde auch das berechtigte Interesse als legitime Rechtsgrundlage erkannt, solange Wesensdaten nicht als besondere Kategorien von personenbezogenen Daten gelten. Dabei wurde ebenso gezeigt, wie eine beispielhafte Interessenabwägung aussehen könnte.

Die Betrachtung des Auskunftsrechts hat ergeben, dass eine Umsetzung des Betroffenenrechts bei BCI in Zukunft möglich sein sollte. Als Herausforderung wurde allerdings herausgearbeitet, dass Daten Dritter vorher aus den Wesensdaten entfernt werden müssen. Es wurde vorgeschlagen, pragmatisch mittels Interessenabwägung damit umzugehen.

Ergänzend hat die Arbeit die Vorgaben zum technischen und organisatorischen Datenschutz geprüft und auf BCI und Wesensdaten angewandt. Dabei wurde festgestellt, dass nach den derzeitigen Regularien bereits etliche sinnvolle Maßnahmen ergriffen werden können, um den Schutz der Daten zu gewährleisten. Beispiele sind hierbei die Verschlüsselung der Daten und der Datenübermittlung sowie die Erkennung von Schadsoftware.

Die Erarbeitung hat im Zuge dessen auch gezeigt, wie datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung bei BCI realisiert werden könnten. Als Nachteil wurde identifiziert, dass diese Vorgaben lediglich für Verantwortliche gelten.

Auf die technischen und organisatorischen Maßnahmen aufbauend wurde ebenso überprüft, ob eine DSFA regelmäßig beim Einsatz von BCI notwendig sein dürfte. Diese Überprüfung kam zu dem Ergebnis, dass in der Regel eine DSFA durchzuführen ist, sobald Wesensdaten verarbeitet werden. Ebenso wurde aufgezeigt, wie genau eine diesbezügliche DSFA aussehen könnte.

Abschließend wurden die Grundlagen der Verarbeitung betrachtet und auf BCI angewandt. Hierbei wurde festgestellt, dass es bereits umfangreiche Möglichkeiten gibt, die grundlegenden Vorgaben, auch bei der Verarbeitung von Wesensdaten, einzuhalten.

Abschließend und zusammenfassend kann demnach dargelegt werden, dass die DSGVO derzeit zwar größtenteils ausreichende Vorgaben beinhaltet, die auch bei der Verarbeitung von Wesensdaten sinnvoll angewendet werden können, allerdings einige bedeutende grundlegende Schwächen aufweist. Besonders erwähnenswert ist dabei die unklare Einordnung von Wesensdaten in den Regulierungsbereich des Art. 9 Abs. 1 DSGVO, die Herausforderungen bei der Einwilligung als Rechtsgrundlage der Verarbeitung und die fehlende allgemeine Verpflichtung bei der Umsetzung von technischen und organisatorischen Datenschutzmaßnahmen. Um diese Regulierungs-Probleme zu beseitigen, wurden einige entsprechende Anpassungsvorschläge gemacht. Besonderes Augenmerk lag dabei auf der Entwicklung eines neuen Systems, bei dem keine Unterscheidung zwischen personenbezogenen Daten und besonderen Kategorien von personenbezogenen Daten mehr besteht. Mit dieser Lösung würde insg. ein besserer Schutz von Wesensdaten gewährleistet werden können. Ebenso wurde vorgeschlagen, dass die bei einer Einwilligung notwendigen Informationen niedrigschwelliger gestaltet und manipulative Einwilligungsmechanismen unterbunden werden sollten. Auch wurde empfohlen, eine allgemeine Verpflichtung bzgl. technischem Datenschutz zu etablieren, sodass auch Hersteller diese Vorgaben einhalten müssten.

2. Weitere rechtliche Implikationen und Forschungsfragen

Diese Arbeit hat sich lediglich mit der datenschutzrechtlichen Betrachtungsweise beschäftigt. BCI werden allerdings nicht nur in diesem Bereich eine Herausforderung sein. Demnach dürften in Zukunft auch noch andere rechtswissenschaftliche Auseinandersetzungen von Interesse sein. Da die Technologie auch auf Künstliche Intelligenz angewiesen ist, dürfte bspw. eine KI-rechtliche[830] Betrachtung ebenso hohe Relevanz haben. Ganz grundsätzlich sind auch verfassungsrechtliche und menschenrechtliche Untersuchungen notwendig. Ebenso könnte die Frage gestellt werden, ob die durch BCI aufgezeichneten Gehirnströme und deren Interpretationen durch eine KI strafrechtlich als Beweismittel fungieren könnten, wie eine Straftat durch Fremdsteuerung einzuordnen ist oder ob ein zivilrechtlicher Vertrag mit Angebot und Annahme auch per Gedanke rechtmäßig stattfinden kann.

Doch auch unabhängig von der Rechtswissenschaft, werfen BCI weitreichende Fragen auf. Es sollte tiefgreifender diskutiert und untersucht werden, welche Auswirkung diese Technologie auf das Verständnis von Menschsein und die Wahrnehmung des Daseins hat. Interessant wäre auch, ob das Leben als lebenswerter empfunden wird, wenn beeinträchtigte Menschen BCI nutzen. Ebenso könnte untersucht werden, inwiefern die exzessive Nutzung eine Auswirkung auf die Psyche und die Morphologie des Gehirns haben könnte. Das sind nur wenige der Fragen, die in Zukunft adressiert werden sollten.

Die Auseinandersetzung mit dieser Thematik steht somit noch am Anfang. Die Metamorphose zum Smart Human wird die gesamte Gesellschaft herausfordern und von der Judikative abverlangen, dass sinnvolle Schutz- und Anpassungsmaßnahmen vorgenommen werden. Schließlich geht es um die Essenz des Menschen, seine Gedanken, sein Bewusstsein – um das, was ihn bis dato von der Maschine unterschieden hat.

830 Siehe EU KI-Verordnung, Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689 (abgerufen 4.1.2025).

Literatur

Abbate, Janet: The Electric Century Getting Small: A Short History of the Personal Computer, Proceedings of the IEEE 1999, S. 1695-1698.

Abdulkader, Sarah N./Atia, Ayman/Mostafa, Mostafa-Sami M.: Brain computer interfacing: Applications and challenges, Egyptian Informatics Journal 2015, S. 213-230.

Acciarini, Chiara/Cappa, Francesco/Boccardelli, Paolo/Oriani, Raffaele: How can organizations leverage big data to innovate their business models? A systematic literature review, Technovation 2023, S. 1-18.

Adamowsky, Natascha: Vom Internet zum Internet der Dinge, in: Florian Sprenger/Christoph Engemann (Hrsg.), Internet der Dinge, Bielefeld 2015, S. 119-135.

Agarwal, Anisha/Dowsley, Rafael/McKinney, Nicholas D./Wu, Dongrui/Lin, Chin-Teng/De Cock, Martine/Nascimento, Anderson C. A.: Protecting Privacy of Users in Brain-Computer Interface Applications, IEEE Transactions on Neural Systems and Rehabilitation Engineering 2019, S. 1546-1555.

Aggrawal, Swati/Chugh, Nupur: Signal processing techniques for motor imagery brain computer interface: A review, Array 2019, S. 1-12.

Agrò, Maurizio: Music and Astronomy, Cham 2023.

Aharoni, Eyal/Vincent, Gina M./Harenski, Carla L./Calhoun, Vince D./Sinnott-Armstrong, Walter/Gazzaniga, Michael S./Kiehl, Kent A.: Neuroprediction of future rearrest, PNAS 2012, S. 6223-6228.

Akindote, Odunayo Josephine/Adegbite, Abimbola Oluwatoyin/Dawodu, Samuel Onimisi/Omotosho, Adedolapo/Anyanwu, Anthony/Maduka, Chinedu Paschal: Comparative review of big data analytics and GIS in healthcare decision-making, World Journal of Advanced Research and Reviews 2023, S. 1293-1302.

Albers, Marion/Veit, Raoul-Darius, 2020, in: Wolff, Heinrich Amadeus/ Brink, Stefan (Hrsg.), Stefan: BeckOK Datenschutzrecht, 36. Aufl.

Albrecht, Jan Philipp/Jotzo, Florian: Das neue Datenschutzrecht der EU, 1. Aufl., Baden-Baden 2017.

Alhazmi, Abdulrahman/Arachchilage, Nalin Asanka Gamagedara: I'm all ears! Listening to software developers on putting GDPR principles into software development practice, Personal and Ubiquitous Computing 2021, S. 879-892.

Al-Nafjan, Abeer/Aldayel, Mashael: Predict Students' Attention in Online Learning Using EEG Data, Sustainability 2022, S. 1-12.

Al-Taair, Suaad Hadi Hassan/Kanber, Huda Abbas/al-Dulaimi, Waleed Abood Mohammed: The Importance of Using the Internet of Things in Education, International Journal of Emerging Technologies in Learning 2023, S. 19-39.

Anderson, Bonnie/Vance, Anthony/Kriwan, Brock/Eargle, David/Howard, Seth: Users Aren't (Necessarily) Lazy: Using NeuroIS to Explain Habituation to Security Warnings, ICIS 2014 Proceedings 2014, S. 1-15.

Andow, Benjamin/Mahmud, Samir Yaseer/Wang, Wenyu/Whitaker, Justin/Enck, William/Reaves, Bradley/Singh, Kapil/Xie, Tao: PolicyLint: Investigating Internal Privacy Policy Contradictions on Google Play, Proceedings of the 28th USENIX Security Symposium 2019, S. 585-602.

Anke, Jürgen/Fischer, Uwe/Lemke, René: Integration digitaler Sprachassistenten in den Kundenservice am Beispiel der Stadtwerke Leipzig, in: Michael Räckers/Sebastian Halsbenning/Detlef Rätz/David Richter/Erich Schweighofer (Hrsg.), Digitalisierung von Staat und Verwaltung, Bonn 2019, S. 25-36.

Aristoteles: Die Kategorien, Stuttgart 2009.

Aristoteles: Die Nikomachische Ethik, Hamburg 1985. (Verlag: Felix Meiner)

Arning, Marian Alexander/Rothkegele, Tobias, 2019, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG, 3. Aufl.

Art.-29-Gruppe: Leitlinien Datenschutz-Folgenabschätzung (DSFA) (WP 248), Brüssel 2017.

Art.-29-Gruppe: Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 (WP 251 1 rev. 01), Brüssel 2017.

Art.-29-Gruppe: Opinion 03/2013 on purpose limitation (WP 203), Brüssel 2013.

Art.-29-Gruppe: Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten (WP 192), Brüssel 2012.

Art.-29-Gruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (WP 136), Brüssel 2007.

Auda, Jonas/Heger, Roman/Kosch, Thomas/Gruenefeld, Uwe/Schneegaß, Stefan: EasyEG: A 3D-printable Brain-Computer Interface, Adjunct Publication of the 33rd Annual ACM Symposium on UIST 2020, S. 70-72.

Bäcker, Matthias, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Baek, Hyun Jae/Chang, Min Hye/Heo, Jeong/Park, Kwang Suk: Enhancing the Usability of Brain-Computer Interface Systems, Computational Intelligence and Neuroscience 2019, S. 1-12.

Bajwa, Garima/Dantu, Ram: Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencepahlograms, Computers & Security 2016, S. 95-113.

Ballsun-Stanton, Brian: Asking About Data, Sydney 2012.

Bansal, Dipali/Mahajan, Rashima: EEG-Based Brain-Computer Interfaces: Cognitive Analysis and Control Applications, London 2019.

Barth, Susanne/de Jong, Menno D.T.: The Privacy Paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, Telematics and Informatics 2017, S. 1038-1058.

Battle-Fisher, Michele: Transhuman, posthuman and complex humanness in the 21th century, Ethics, Medicine and Public Health 2020, S. 1-8.

Baumgartner, Ulrich, 2018, in: Ehmann, Eugen/ Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung DS-GVO.

Baumgartner, Ulrich/Gausling, Tina: Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen – Was Unternehmen jetzt nach der DS-GVO beachten müssen, ZD 2017, S. 308-313.

Bechmann, Anja: Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook, Journal of Media Business Studies 2014, S. 21-38.

Beck, Laura: BIM im Facility Management, Wiesbaden 2023.

Benjumea, Jaime/Ropero, Jorge/Rivera-Romero, Octavio/Dorronzoro-Zubiete, Enrique/Carrasco, Alejandro: Assessment of the Fairness of Privacy Policies of Mobile Health Apps: Scale Development and Evaluation in Cancer Apps, JMIR Mhealth Uhealth 2020, S. 1-20.

Bensch, Michael/Karim, Ahmed A./Mellinger, Jürgen/Hinterberger, Thilo/Tangermann, Michael/Bogdan, Martin/Rosenstiel, Wolfgang/Birbaumer, Niels: Nessi: An EEG-Controlled Web Browser for Severly Paralyzed Patients, Computational Intelligence and Neuroscience 2007, S. 1-5.

Berger, Hans: Über das Elektrenkephalogramm des Menschen. Archiv für Psychiatrie und Nervenkrankheiten 1929, S. 527-570.

Bergram, Kristoffer/Bezencon, Valery/Maingot, Paul/Gjerlufsen, Tony/Holzer, Adrian: Digital Nudges for Privacy Awareness: From consent to informed consent?, ECIS 2020 Research Papers 2020, S. 1-16.

Bernal, Sergio Lopez/Celedrán, Alberto Huertas/Pérez, Gregorio Martínez/Barros, Michael Taynnan/Balasubramaniam, Sasitharan: Security in Brain-Computer Interfaces: State-Of-The-Art, Opportunities, and Future Challenges, ACM Computing Surveys 2022, S. 1-31.

*Beyer, Reinhard/*Gerlach, *Rebekka:* Sprache und Denken, 2. Aufl., Wiesbaden 2018.

Binnendijk, Anika/Marler, Timothy/Bartels, Elizabeth M.: Brain-Computer Interfaces U.S. Military Applications and Implications, Kalifornien 2020.

Birbaumer, N./Ghanayim, N./Hinterberger, T./Iversen, I./Kotchoubey, B./Kübler, A./Perelmouter, J./Taub, E./Flor, H.: A spelling device for the paralysed, Nature 1999, S. 297-298.

Bitkom: Datenschutz in der digitalen Welt, Berlin 2015.

Bitkom: DS-GVO und Corona – Datenschutzherausforderungen für die Wirtschaft, Berlin 2020.

Bitkom: Leitlinien für den Big-Data-Einsatz, Berlin 2015.

Bockbrader, Marcia: Upper limb sensorimotor restoration through brain–computer interface technology in tetraparesis, Current Opinion in Biomedical Engineering 2019, S. 85-101.

Boehme-Neßler, Volker: Das Ende der Anonymität, Datenschutz und Datensicherheit 2016, S. 419-423.

Boehme-Neßler, Volker: Gläserne Prostituierte?, DuD 2019, S. 342-346.

Boehme-Neßler, Volker: Pictoral Law, Heidelberg 2011.

Boehme-Neßler, Volker: Privacy: a matter of democracy. Why democracy needs privacy and data protection, International Data Privacy Law 2016, S. 222-229.

Bogard, William: Welcom to the Society of Control: The Simulation of Surveillance Revisited, in: Kevin D Haggerty/Richard V. Ericson (Hrsg), The New Politics of Surveillance and Visibility, Toronto 2006, S. 55-78.

Bonaci, Tamara/Calo, Ryan/Chizeck, Howard Jay: App Stores for the Brain: Privacy and Security in Brain-Computer Interfaces, IEEE Technology and Society Magazine 2015, S. 32-39.

Bonnet, Laurent/Lotte, Fabien/Lécuyer, Anatole: Two Brains, One Game: Design and Evaluation of a Multiuser BCI Video Game Based on Motor Imagery, IEEE Transactions on Computational Intelligence and AI in Games 2013, S. 185-198.

Bousseta, R./El Ouakouak, I./Gharbi, M./Regragui, F.: EEG Based Brain Computer Interface for Controlling a Robot Arm Movement Through Thought, IRBM 2018, S. 129-135.

boyd, danah/Crawford, Kate: Critical Questions for Big Data, Information, Communication & Society 2012, S. 662-679.

Bravo-Lillo, Cristian/Komanduri, Saranga/Cranor, Lorrie Faith/Reeder, Robert W./ Sleeper, Manya/Downs, Julie/Schechter, Stuart: Your attention please: designing security-decision UIs to make genuine risks harder to ignor, Proceedings of the Ninth Symposium on Usable Privacy and Security 2013, S. 1-12.

Brennan, Emily/Maloney, Erin K./Ophir, Yotam/Cappella, Joseph: Potential Effectiveness of Pictorial Warning Labels That Feature the Images and Personal Details of Real People Nicotine & Tobacco Research 2017, S. 1138-1148.

Brink, Stefan/Eckhardt, Jens: Wann ist ein Datum ein personenbezogenes Datum? Anwendungsbereich des Datenschutzrechts, ZD 2015, S. 205-212.

Browning, John G./Tuma, Shawn: If Your Heart Skips a Beat, it May Have Been Hacked: Cyber Security Concerns with Implanted Medical Devices, South Carolina Law Review 2016, S. 637-677.

Brusseau, James: Mapping AI avant-gardes in time: posthumanism, transhumanism, genhumanism, Discover Artificial Intelligence 2023, S. 1-11.

Buchner, Benedikt/Petri, Thomas, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Buchner, Benedikt/Tinnfeld, Marie-Theres, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Cabañas, José González/Cuevas, Ángel/Arrate, Aritz/Cuevas, Rubén: Does Facebook Use Sensitive Data for Advertising Purposes?, Communications of the ACM 2021, S. 62-69.

Cao, Lei/Li, Jei/Li, Hongfei/Jiang, Changjun: A hybrid brain computer interface system based on neurophysiological protocol and brain-actuated switch for wheelchair control, Journal of Neuroscience Methods 2014, S. 33-43.

Caton, Richard: The electrical currents of the brain, British Medical Journal 1875, S. 278.

Chen, Min/Mao, Shiwen/Liu, Yunhao: Big Data: A Survey, Mobile Networks and Applications 2014, S. 171-209.

Chester, Jeff/Montgomery, Kathryn C.: The role of digital marketing in political campaigns, Internet Policy Review 2017, S. 1-20.

Chester, Jeff/Montgomery, Kathryn C.: The role of digital marketing in political campaigns, Internet Policy Review 2017, S. 1-20.

Chi, Nguyen Thi Khanh/Vu, Nam Hoang: Investigating the customer trust in artificial intelligence: The role of anthropomorphism, empathy response, and interaction, CAAI Transactions on Intelligence Technology 2023, S. 260-273.

Chittaranjan, Gokul/Blom, Jan/Gatica-Perez, Daniel: Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones, IEEE 2011, S. 29-36

Christl, Wolfie: Kommerzielle digitale Überwachung im Alltag, Wien 2014.

Christl, Wolfie: Microtargeting: Persönliche Daten als politische Währung, Aus Politik und Zeitgeschichte 2019, S. 42-48.

Cinel, Caterina/Valeriani, Davide/Poli, Riccardo: Neurotechnologies for Human Cognitive Augmentation: Current State of the Art and Future Prospects, Frontiers in Human Neuroscience 2019, S. 8-24.

Clément, Claude: Brain-Computer Interface Technologies, Cham 2019.

Culik, Nicolai/Döpke, Christian: Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwednungen, ZD 2017, S. 226-230.

Danezis, George/Domingo-Ferrer, Josep/Hansen, Marit/Hoepman, Jaap-Henk/Le Métayer, Rodica Tirtea/Schiffner, Stefan: Privacy and Data Protection by Design – from policy to enginee-ring, Athen 2014.

Das, Gitanjali/Cheung, Cynthia/Nebeker, Camille/Bietz, Matthew/Bloss, Cinnamon: Privacy Policies for Apps Targeted Toward Youth: Descriptive Analysis of Readability, JMIR Mhealth Uhealth 2018, S. 1-12.

Datenschutzkonferenz: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019.

Deloitte: Smart Home Consumer Survey 2018, München, 2018.

Denning, Tamara/Matsuoka, Yoky/Kohno, Tadayoshi: Neurosecurity: security and privacy for neural devices, Journal of Neurosurgery 2009, S. 1-4.

Dessauer, Friedrich: Philosophie der Technik, Bonn 1927.

Ditai, J./Kanyago, J./Nambozo, M. R./Odeke, N.M./Abeso, J./Dusabe-Richards, J./Olupot-Olupot, P./Carrol, E. D./Medina-Lara, A./Gladstone, M./Storr, J./Faragher, B./Weeks, A. D.: Optimising informed consent for participants in a randomised controlled trial in rural Uganda: a comparative prospective cohort mixed-methods study, Trials 2018, S. 1-11.

Dix, Alexander, 2019, in: Smitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht DSGVO mit BDSG, 1. Aufl.

Dong, Yuanrui/Wang, Shirong/Huang, Qiang/Berg, Rune W./Li, Guanghui/He, Jiping: Neural Decoding for Intercortical Brain-Computer Interfaces, Cyborg and Bionic Systems 2023, S. 1-12.

Drew, Liam: Decoding the business of brain-computer interfaces, Nature Electronics 2023, S. 90-95.

Droste, Wiebke/Hoffmann, Klaus-Peter/Olze, Heidi/Kneist, Werner/Krüger, Thilo/Rupp, Rüdiger/Ruta, Marc: Interactive Implants: Ethical, legal and social implications, Current Directions in Biomedical Engineering 2018, S. 1-16.

EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Brüssel 2020 (Version 2.0).

Emanuel, Ezekiel J./Boyle, Connor W.: Assessment of Length and Readability of Informed Consent Documents for COVID-19 Vaccine Trials, JAMA Network Open 2021, S. 1-5.

Engels, Barbara/Grunewald, Mara: Das Privacy Paradoxon: Digitalisierung versus Privatsphäre, IW-Kurzberichte 2017, S. 1-3.

Engels, Barbara: Datenschutzpräferenzen von Jugendlichen in Deutschland, IW-Trends 2018, S. 3-26.

Erden, Yasemin J./Brey, Philip: Neurotechnology and ethics guidelines for human enhancement: The case of the hippocampal cognitive prosthesis, Artificial Organs 2023, S. 1235-1241.

Ernst, Stefan, 2021, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl.

Europäische Kommission: Special Eurobarometer 487a: The General Data Protection Regulation, Brüssel 2019.

Faaique, Muhammad: Overview of Big Data Analytics in Modern Astronomy, Internation Journal of Mathematics, Statistics, and Computer Science 2024, S. 96-113.

Farahany, Nita A.: Incriminating Thoughts, Stanford Law Review 2011, S. 11-17.

Ferracuti, Francesco/Iarlori, Sabrina/Mansour, Zahra/Monteriù, Andrea/Porcaro, Camillo: Comparing between Different Sets of Preprocessing, Classifiers, and Channels Selection Techniques to Optimise Motor Imagery Pattern Classification System from EEG Pattern Recognition, Brain Sciences 2022, S. 1-16.

Fichte, Johann Gottlieb: Grundlagen des Naturrechts und Principien der Wissenschaftslehre Jena/Leipzig 1796.

Filippi, Massimo/Riccitelli, Gianna/Falini, Andrea/Di Salle, Francesco/Vuilleumier, Patrik/Comi, Giancarlo/Rocca, Maria A.: The Brain Functional Networks Associated to Human and Animal Suffering Differ among Omnivores, Vegetarians and Vegans, PLoS One 2010, S. 1-9.

Forbrukerrådet: Deceived by Design, Oslo 2018.

Franck, Lorenz, 2018, in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl.

Franzen, Martin, 2018, in: Franzen, Martin/Gallner, Inken/Oetker, Hartmut (Hrsg.): Kommentar zum europäischen Arbeitsrecht, 2. Aufl.

Frege, *Gottlob:* Der Gedanke. Eine logische Untersuchung, Beiträge zur Philosophie des deutschen Idealismus 1918-1919, S. 58-77.

Frenzel, Eike Michael, 2021, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl.

Gandy, Oscar: Data Mining, Surveillance, and Discrimination in the Post-9/11 Enviroment, in: Kevin D. Haggerty/Richard V. Ericson (Hrsg), The New Politics of Surveillance and Visibility, Toronto 2006, S. 363-384.

Gasson, Mark N./Koops, Bert-Jaap: Attacking Human Implants: A New Generation of Cybercrime, Law, Innovation and Technology 2013, S. 248-277.

Glaser, Barney G.: All is Data, The Grounded Theory Review 2007, S. 1-22.

Gluck, Joshua/Schaub, Florian/Friedman, Amy/Habib, Hana/Sadeh, Norman/Cranor, Lorrie Faith/Agarwal, Yuvraj: How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices, Proceedings of the Twelfth Symposium on Usable Privacy and Security 2016, S. 321-340.

Gola, Peter, 2018, in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl.

Gola, Peter/Schomerus, Rudolf, 2012, in: Gola, Peter/Schomerus, Rudolf (Hrsg.)/ Schomerus, Rudolf (Hrsg.): BDSG Bundesdatenschutzgesetz, 11. Aufl.

Gräßler, Florian: War die DDR totalitär?, Baden-Baden 2014.

Greenberg, Anastasia: Inside the Mind's Eye: An International Perspective on Data Privacy Law in the Age of Brain-Machine Interfaces, Journal of Science and Technology 2019, S. 79-122.

Greve, Holger, 2020, in: Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (Hrsg.): DSGVO BDSG, 7. Aufl.

Groves, Katie/Kennett, Steffan/Gillmeister, Helge: Evidence for ERP biomarkers of eating disorder symptoms in women, Biology Psychology 2017, S. 205 - 219.

Grübler, Gerd/Hildt, Elisabeth/Various Authors: The User's Perspective, in: Gerd Grübler/Elisabeth Hildt (Hrsg.), Brain-Computer Interfaces in their ethical, social and cultural contexts, Dordrecht 2014, S. 115-126.

Guger, Christoph/Allison, Brendan Z./Edlinger, Günther: Emerging BCI Opportunities from a Market Perspective, in: Gerd Grübler/Elisabeth Hildt (Hrsg.), Brain-Computer Interfaces in their ethical, social and cultural contexts, Dordrecht 2014, S. 85-98.

Guger, Christoph/Allison, Brendan Z./Mrachacz-Kersting, Natalie: Brain-Computer Interface Research: A State-of-the-Art Summary 7, in: Christoph Guger/Brendan Z. Allison/Natalie Mrachacz-Kersting (Hrsg.), Brain-Computer Interface Research, Cham 2019, S. 1-10.

Guger, Christoph/Ince, Nuri Firat/Korostenskaja, Milena/Alloson, Brendan Z.: Brain-Computer Interface Research: A State-of-the-Art Summary 11, in: Christoph Guger, Bendan Allison, Tomasz M. Rutkowski, Milena Korostenskaja (Hrsg.), Brain-Computer Interface Research, Cham 2024, S. 1-11.

Hallinan, Dara/Schütz, Philip/Friedewald, Michael/de Hert, Paul: Neurodata and Neuroprivacy: Data Protection Outdated?, Surveillance & Society 2014, S. 55-72.

Hallinan, Dara/Schütz, Philip/Friedewald, Michael/de Hert, Paul: Neurodata and Neuroprivacy: Data Protection Outdated?, Surveillance & Society 2014, S. 55-72.

Hammilton, Lisa Dawn/Meston, Cindy M.: Differences in Neural Response to Romatic Stimuli in Monogamous and Non-Monogamous Men, Archive of Sexual Behavior 2017, S. 2289-2299.

Hansen, Marit, 2019, in: Smitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht DSGVO mit BDSG, 1. Aufl.

Hansen, Marit, 2020, in: Wolff, Heinrich Amadeus/ Brink, Stefan (Hrsg.), Stefan: BeckOK Datenschutzrecht, 36. Aufl.

Hartung, Jürgen, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Hassija, Vikas/Chamola, Vinay/Bajpai, Balindam Chandra/Zeadall, Naren/Zeadally, Sherali: Security Issues in Implantable Medical Devices: Fact or Fiction, Sustainable Cities and Society 2020, S. 1-12.

Haynes, John-Dylan/Sakai, Katsuyuki/Rees, Geraint/Gilbert, Sam/Frith, Chris/Passingham, Richard E.: Reading Hidden Intentions in the Human Brain, Current Biology 2007, S. 323-328.

Heberlein, Horst, 2018, in: Ehmann, Eugen/ Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung DS-GVO.

Hellmann, Roland: IT-Sicherheit, Berlin 2018.

Herbst, Tobias, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Herweg, Andreas/Gutzeit, Julian/Kleih, Sonja/Kübler Andrea: Wheelchair control by elderly participants in a virtual enviroment wtih a brain-computer interface (BCI) and tactile stimulation, Biological Psychology 2016, S. 117-124.

Hladjk, Jörg, 2018, in: Ehmann, Eugen/ Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung DS-GVO.

Hobbes, Thomas: Leviathan, Hamburg 1996.

Hochberg, Leigh R./Anderson, Kim D.: BCI Users and their Needs, , in: Jonathan R. Wolpaw/Elizabeth Winter Wolpaw (Hrsg.), Brain-Computer Interfaces, Oxford 2012, S. 317-323.

Hofmann, Kai/Hornung, Gerrit: Rechtliche Herausforderungen des Internets der Dinge, in: Florian Sprenger/Christoph Engemann (Hrsg.), Internet der Dinge, Bielefeld 2015, S. 181-203.

Hossain, Khondoker Murad/Islam, Md. Ariful/Hossain, Shahera/Nijholt, Anton/Ahad, Md Atiqur Rahman: Status of deep learning for EEG-based brain-computer interface applications, Frontiers in Computational Neuroscience 2023, S. 1-17.

Hoy, Matthew B.: Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants, Medical Reference Services Quarterly 37, S. 81-88.

Huckvale, Kit/Torous, John/Larsen, Mark E.: Assesment oft he Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation, JAMA Network Open 2019, S. 1-10.

Hume, David: Eine Untersuchung über den menschlichen Verstand, 6. Aufl., Leipzig 1097.

Humphreys, *Rebekah:* Animals, Ethics, and Language, Cham 2023.

Ienca, Marcello/Andorno, Roberto: Towards new human rights in the age of neuroscience and neurotechnology, Life Sciences, Society and Policy 2017, S. 1-27.

Ienca, Marcello/Haselager, Pim: Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity, Ethics and Information Technology 2016, S. 117-129.

Ienca, Marcello/Malgieri, Gianclaudio: Mental data protection and the GDPR, Journal of Law and the Biosciences 2022, S. 1-19.

International Telecommunication Union: Overview of the Internet of Things, Geneva 2013.

International Telecommunication Union: Overview of the Internet of Things, Geneva 2013.

Islam, Nayeem/Want, Roy: Smartphones: Past, Present and Future, PERVASIVE computing 2014, S. 89-92.

Jade, Laura/Gentle, Sam: New Ways of Knowing Ourselves. BCI Facilitating Artistic Exploration of Our Biology, in: Anton Nijholt (Hrsg.), Brain Art, 2019, S. 229-262.

Jana, Gopal Chandra/Swetapadma, Aleena/Pattnaik, Prasant Kumar: Enhanching the performance of motor imagery classifivation to design a robust brain computer interface using feed forward back-propagation neural network, Ain Shams Engineering Journal 2018, S. 2871-2878.

Jandt, Silke, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Jiang, Linxing/Stocco, Andrea/Losey, Darby M,/Abernethy, Justin A./Prat Cantel S./Rao, Rajesh P. N.: BrainNet: A Multi-Person Brain-to-Brain Interface for Direct Collaboration Between Brains, Scientific Reports 2019, S. 1-11.

Jöns, Johanna: Daten als Handelsware, Hamburg 2016.

Kamiya, Joe: Operant control of the EEG alpha rhythm and some of its reported effects, in: Charles Tart (Hrsg.), Altered States of Consciousness: A Book of Readings, New York 1969, S. 489–501.

Kamlah, Wulf, 2018, in: Plath, Kai-Uwe (Hrsg.): DSGVO BDSG, 3. Aufl.

Kampert, David, 2018, in: Sydow (Hrsg.), Gernot: Europäische Datenschutzgrundverordnung, 2. Aufl.

Kant, Immanuel: Die Metaphysik der Sitten, 2. Aufl., Berlin 2013.

Karg, Moritz, 2019, in: Smitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht DSGVO mit BDSG, 1. Aufl.

Karikari, Evelyn/Koshechkin, Konstantin A.: Review on brain-computer interface technologies in healthcare, Biophysical Reviews 2023, S. 1351-1358.

Kasera, Shruti/Gehlot, Anita/Uniyal, Varibhav/Pandey, Shweta/Chhabra, Gunjan/Joshi, Kapil: Right to Digital Privacy: A Technological Intervention of Blockchain and Big Data Analytics, 2023 International Conference on Innovative Data Communication Technologies and Application 2023, S. 1122-1127.

Kawala-Sterniuk, Aleksandra/Browarska, Natalia/Al-Bakri, Amir/Pelc, Mariusz/Zygarlicki, Jaroslaw/Sidikova, Michaeleá/Matinek, Radek/Gorzelanczyk, Edward Jacek: Summary of over Fifty Years with Brain-Computer Interfaces – A Review, Brain Sciences 2021, S. 1-41.

Kim, Joohee/Im, Il: Anthropomorphic response: Understanding interactions between humans and artificial intelligence agents, Computers in Human Behavior 2023, S. 1-19.

Klabunde, Achim, 2018, in: Ehmann, Eugen/ Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung DS-GVO.

Klar, Manuel/Kühling, Jürgen, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Klement, Jan Henrik, 2019, in: Smitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht DSGVO mit BDSG, 1. Aufl.

Knierim, Michael Thomas/Bleichner, Martin Georg/Reali, Pierluigi: A Systematic Comparison of High-End and Low-Cost EEG Amplifiers for Concealed, Around-the-Ear EEG Recordings, Sensors 2023, S. 1-23.

Knutson, Kristine M./Mah, Linda/Manly, Charlotte F./Grafman, Jordan: Neural Correlates of Automatic Beliefs About Gender and Race, Human Brain Mapping 2007, S. 915-930.

Kohli, Varun/Tripathi, Utkarsh/Camola, Vinay/Rout, Bijay Kumar/Kanhere, Salil S.: A review on Virtual Reality and Augmented Reality use-cases of Brain Computer Interface based applications for smart cities, Microprocessors and Microsystems 2022, S. 1-13.

Korovesis, Nikolaos/Kandris, Dionisis/Koulouras, Grigorios/Alexandridis, Alex: Robot Motion Control via an EEG-Based Brain-Computer Interface by Using Neural Networks and Alpha Brainwaves, Electronics 2019, S. 1-16.

Kosinski, Michal/Stillwell, David/Graepelb, Thore: Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, PNAS 2013, S. 5802-5805.

Kosinski, Michal/Stillwell, David/Greapel, Thore: Private traits and attributes are predictable from digital records of human behavior, PNAS 2013, S. 5802-5805.

Kosinski, Michal/Stillwell, David/Kohli, Pushmeet/Bachrach, Yoram/Graepel, Thore: Personality and Website Choice, ACM Web Sciences 2012, S. 1-4.

Kosmyna, Nataliya/Lécuyer, Anatole: A conceptual space for EEG-based brain-computer interfaces, PLoS One 2019, S. 1-30.

Kosmyna, Nataliya/Tarpin.Bernard, Franck/Bonnefond, Nicolas/Rivet, Bertrand: Feasibility of BCI Control in a Realistic Smart Home Envirmonment, Frontiers in Human Neuroscience 2016, S. 1-10.

Krishna, S. Rama/Rathor, Ketan/Ranga, Jarabala/Soni, Anita/D, Srinivas/Kumar N, Anil: Artificial Intelligence Integrated with Big Data Analytics for Enhanced Marketing, 2023 International Conference on Inventive Computation Technologies 2023, S. 1073-1077.

Krohm, Niclas: Abschied vom Schriftformgebot der Einwilligung Lösungsvorschläge und künftige Anforderungen, ZD 2016, S. 368-373.

Kronemann, Bianca/Kizgin, Hatice/Rana, Nripendra/Dwivedi, Yogesh K.: How AI encourages consumers to share their secrets? The role of anthropomorphism, personalisation, and privacy concerns and avenues for future research, Spanish Journal of Marketing 2023, S. 3-19.

Krusienski, Dean J./McFarland, Dennis J./Principe, José C.: BCI Signal Processing: Feature Extraction, in: Jonathan R. Wolpaw/Elizabeth Winter Wolpaw (Hrsg.), Brain-Computer Interfaces, Oxford 2012, S. 123-145.

Landau, Ofir/Cohen, Aviad/Gordon, Shirley/Nissim, Nir: Mind your privacy: Privacy leakage through BCI applications using machine learning methods, Knowledge-Based Systems 2020, S. 1-21.

Landau, Ofir/Puzis, Rami/Nissim, Nir: Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space, ACM Computing Surveys 2020, S. 1-38.

Lang, Markus, 2019, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG, 4. Aufl.

Latini, Sara: To the edge of data protection: How brain information can push the boundaries of sensitivity, Tilburg 2018.

Laue, Philip, 2019, in: Spindler, Gerald/Schuster, Fabian: Recht der elektronischen Medien, 4. Aufl.

Lee, Hongmi/Kuhl, Brice A.: Reconstructing Perceived and Retrieved Faces from Activity Patterns in Lateral Parietal Cortex, The Journal of Neuroscience 2016, S. 6069-6082.

Li, Xin/Feng, Min/Ran, Youhua/Su, Yang/Liu, Feng/Huang, Chunlin/Shen, Huanfeng/Xiao, Qing/Su, Jianbin/Yuan, Shinwei/Guo, Huadong: Big Data in Earth system science and progress towards a digital twin, Nature Reviews Earth & Environment 2023, S. 319-332.

Liang, Fan/Das, Vishnupriya/Kostyuk, Nadiya/Hussain, Muzammil M.: Constructiong a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure, Policy & Internet 2018, S. 415-453.

Lilley, Stephen: Transhumanism and Society, New York 2013.

Lim, Choon Guan/Soh, Chui Pin/Lim, Shernice Shi Yun/Fung, Daniel Shuen Sheng/Guan, Cuntai/Lee, Tih-Shih: Home-based brain–computer interface attention training program for attention defcit hyperactivity disorder: a feasibility trial, Child and Adoleschent Psychiatry and Mental Health 2023, S. 1-11.

Lindegren, Daniel/Karegar, Farzaneh/Kane, Bridget/Pettersson, John Sören: An evaluation of three designs to engage users when providing their consent on smartphones, Behaviour & Information Technology 2019, S. 398-414.

Liu, Hong: Philosophical Reflections on Data, Procedia Computer Science 2014, S. 60-65.

Liyanage, S. R./Bhatt, Chintan: Wearable electroencephalography technologies for brain-computer interfacing, in: Nilanjan Dey/Amira S. Shour/Simon James Fong, Wearable and Implantable Medical Devices, London 2020, S. 55-78.

Loukides, Grigorios/Denny, Joshua C./Malin, Bradley: The disclosure of diagnosis codes can breach research participants' privacy, Journal oft he American Medical Informatics Association 2010, S. 322 (323 ff.).

Loy, Carolin/Baumgartner, Ulrich: Consent-Banner und Nudging, ZD 2021, S. 404-408.

Machuletz, Dominique/Böhme, Rainer: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR, Proceedings in Privacy Enhanching Technologies 2020, S. 481-498.

Magee, Patrick/Ienca, Marcello/Farahany, Nita: Beyond neural data: Cognitive biometrics and mental privacy, Neuron 2024, S. 3017-3028.

Mahmood, Musa/Mzurikwao, Deogratias/Kim, Yun-Soung/Lee, Yongkuk/Mishra, Saswat/Herbert, Robert/Duarte, Audrey/Ang, Chee Siang/Yeo, Woon-Hong: Fully portable and wireless universal brain-machine interfaces enabled by flexible scalp electronics and deep learning algorithm, Nature Machine Intelligence 2019, S. 412-422.

Mailseli, Baraka/Abdall, Abdi T./Massawe, Liebe V./Mbise, Mercy/Mkocha, Khadija/Nassor, NAssor Ally/Ismail, Moses/Michael, James/Kimambo, Samwel: Brain-computer interface: trend, challenges, an threats, Brain Informatics 2023, S. 1-16.

Mak, Joseph N./Wolpaw, Jonathan R.: Clinical Applications of Brain-Computer Interfaces: Current State and Future Prospects, IEEE Reviews in Biomedical Engineering 2009, S. 187-199.

Malgieri, Gianclaudio/Comandé, Giovanni: Sensitive-by-distance: quasi-health data in the algorithmic era, Information & Communications Technology Law 2017, S. 229-249.

Mantz, Reto, 2018, in: Sydow (Hrsg.), Gernot: Europäische Datenschutzgrundverordnung, 2. Aufl.

Martini, Mario, 2021, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl.

Martini, Mario/Drews, Christian/Seeliger, Paul/Weinzierl, Quirin: Dark Patterns, ZfDR 2021, S. 47-74.

Martini, Mario/Kemper, Carolin: Cybersicherheit von Gehirn-Computer-Schnittstellen, International Cybersecurity Law Review 2022, S. 191-243.

Martinovic, Ivan/Davies, Doug/Frank, Mario/Perito, Daniele/Ros, Tomas/Song, Dawn: On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces, Proceedings of the 21st USENIX Security Symposium 2012, S. 1-16.

Mattia, Donnatella/Molinari, Marco: Brain-Computer Interfaces and Therapy, in: Gerd Grübler/Elisabeth Hildt (Hrsg.), Brain-Computer Interfaces in their ethical, social and cultural contexts, Dordrecht 2014, S. 49-59.

McCane, Lynn M./Heckmann, Susan M./McFarland, Dennis J./Townsend, George/Mak, Joseph N./Sellers, Eric W./Zeitlin, Debra/Tenteromano, Laura M./Wolpaw Jonathan R./Vaughan, Theresa M.: P300-based brain-computer interface (BCI) event-related potentials (ERPs): People with amyotrophic lateral sclerosis (ALS) vs. Age-matched controls, Clinical Neurophysiology 2015, S. 2124-2131.

McCullagh, Karen: Data Sensitivity: Proposals of Resovling the Conundrum, Journal of International Commercial Law and Technology 2007, S. 190-201.

McDonald, Aleecia M./Cranor, Lorrie Faith: The Cost of Reading Privacy Policies, A Journal of Law and Policy oft he Information Society 2008, S. 543-568.

McFarland, D. J./Wolpaw, J. R.: EEG-based brain–computer interfaces, Current Opinion in Biomedical Engineering 2017, S. 194-200.

McFarland, Dennis J./Krusienski, Dean J.: BCI Signal Processing: Feature Translation, in: Jonathan R. Wolpaw/Elizabeth Winter Wolpaw (Hrsg.), Brain-Computer Interfaces, Oxford 2012, S. 147-163.

Mehta, Ranjana K./Parasuraman, Raja: Neuroergonomics: a review of applications to physical and cognitive work, Frontiers in Human Neuroscience 2013, S. 1-10.

Mester, Britta Alexandra, 2019, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG, 3. Aufl.

Meyer, Hermann Joseph: Die Technisierung der Welt, Tübingen 1961.

Millet, David: Hans Berger: From Psychic Energy to the EEG, Perspectives in Biology and Medicine 2001, S. 522-542.

Miralles, Felip/Vargiu, Eloisa/Dauwalder, Stefan/Solà, Marc/Müller-Pütz, Gernot/Wriesnegger, Selina C./Pinegger, Andreas/Kübler, Anderea/Halder, Sebastian/Käthner, Ivo/Martin, Suzanne/Daly, Jean/Armstrong, Elaine/Guger, Christoph/Hintermüller, Christoph/Lowish, Hannah: Brain Computer Interface on Track to Homes, The Scientific World Journal 2015, S. 1-17.

Moore Jackson, Melody/Mappus, Rudolph: Applications for Brain-Computer Interfaces, in: Desney Tan/Anton Nijholt (Hrsg.), Brain Computer Interfaces Applying our Minds to Human-Computer Interaction, London 2010, S. 89-104.

Morales-Trujillo, Miguel Ehécatl/García-Mireles, Gabriel Alberto/Matla-Cruz, Erick Orlando/Piattini, Mario: A Systematic Mapping Study ofPrivacy by Design in Software Engineering, CLEI Electronic Journal 2019, S. 1-29.

Moses, David A./Leonard, Matthew K./Makin, Joseph G./Chang, Edward F.: Real-time decoding of question-and-answer speech dialogue using human cortical activity, Nature Communications 2019, S. 1-14.

Mugdal, Shiv Kumar/Sharma, Suresh K/Chaturvedi, Jitender/Sharma, Anil: Brain computer interface advancement in neurosciences: Applications and issues, Interdisciplinary Neurosurgery 2020, S. 1-8.

Mugler, Emily M./Ruf, Carolin A./Halder, Sebastian/Bensch, Michael/Kübler, Andrea: Design and Implementation of a P300-Based Brain-Computer Interface for Controlling an Internet Browser, IEEE Transactions on Neural Systems and Rehabilitation Engineering 2010, S. 599-609.

Musk, Elon/Neuralink: An Integrated Brain-Machine Interface Platform with Thousands of Channels, 2019.

Müßinger, Jana I./Halder, Sebastian/Kleih, Sonja C./Furdea, Adrian/Raco, Valerio/Hösle, Adi/Kübler, Andrea: Brain Painting: first evaluation of a new brain-computer interface application with ALS-patients and healthy volunteers, Frontiers in Neuroscience 2010, S. 1-11.

Nagel, Thomas: What Is It Like to Be a Bat?, The Philosophical Review 1974, S. 435-450.

Nemrodov, Dan/Niemeier, Matthias/Patel, Ashutosh/Nestor, Adrian: The Neural Dynamics of Facial Identity Processing: Insights from EEG-Based Pattern Analysis and Image Reconstruction, eNeuro 2018, S. 1-17.

Nestor, Liam J./McCabe, Ella/Jones, Jennifer/Clancy, Luke/Garavan, Hugh: Smokers and ex-smokers have shared differences in the neural substrates for potential monetary gains and losses, Addiction Biology 2016, S. 369 (375 ff.).

Neves, Flávio/Souza, Rafael/Sousa, Juliana/Bonfim, Michel/Garcia, Vinicius: Data privacy in the Internet of Things based on anonymization: A review, Journal of Computer Security 2023, S. 261-291.

Niedermann, Anne: IfD-Umfrage 8201, Freiwillige und informierte Einwilligung? Die Nutzerperspektive, Allensbacher Archiv 2019, S. 1-11.

Nijboer, F./Sellers, E.W./Mellinger, J./Jordan, M. A./Matuz, T./Furdea, A./Halder, S./Mochty, U./Krusienski, D. J./Vaughan, T. M./Wolpaw, J. R./Birbaumer, N./Kübler, A.: A P300-based brain-computer interface for people with amyotrophic lateral sclerosis, Clinical Neurophysiology 2008, S. 1909-1916.

Nink, Judith, 2019, in: Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 4. Aufl.

Nishimoto, Shinji/Vu, An T./Naselaris, Thomas/Benjamini, Yuval/Yu, Bin/Gallant, Jack L.: Reconstructing Visual Experiences from Brain Activity Evoked by Natural Movies, Current Biology 2011, S. 1641-1646.

Nolte, Norbert/Werkmeister, Christopher, 2018, in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl.

Nomura, Tomomi/Mitsukura, Yasue: EEG-Based Detection of TV Commercials Effects, Procedia Computer Science 2015, S. 131-140.

Nouwens, Midas/Liccardi, Ilaria/Veale, Michael/Karger, David/Kagal, Lalana: Dark patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, Proceedings of the 2020 CHI Conference in Human Factors in Computing Systems 2020, S. 1-13.

Nyholm, Sven: Artificial Intelligence and Human Enhancement: Can AI Technologies Make Us More (Artificially) Intelligent?, Cambridge Quarterly of Healthcare Ethics 2023, S. 76-88.

Obar, Jonathan A./Oeldorf-Hirsch, Anne: The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, Information, Communication & Society 2016, S. 1-20.

OECD, Skills Matter: Additional Results from the Survey of Adult Skills, Paris 2019.

Oettel, Maurice: Einwilligung per Gedanke, PinG 2022, S. 136-138.

Oettel, Maurice: Smart Human und der Schutz der Gedanken, DuD 2020, S. 386-389.

Oettel, Maurice: Wesensdaten: Regulierungslücke im derzeitigen Datenschutzrecht, DuD 2021, S. 632-626.

Ohlhorst, Frank: Big Data Analytics, Hoboken 2013.

Olson, Karin: What Are Data? Qualitative Health Research 2021, S. 1567-1569.

Opaschowski, Horst W.: Die Wünsche der Verbraucher, in: Helmut Bäumler/Albert von Mutius, Datenschutz als Wettbewerbsvorteil, 1. Aufl., Braunschweig 2002, S. 13-19.

Orban, Mostafa/Elsamanty, Mahmoud/Guo, Kai/Zhang, Senhao/Yang, Hongbo: A Review of Brain Activity and EEG-Based Brain–Computer Interfaces for Rehabilitation Application, Bioengineering 2022, S. 1-22.

Otto, Kevin J./Ludwig, Kip A./Kipke, Daryl R.: BCI Design, Implementation, and Operation, in: Jonathan R. Wolpaw/Elizabeth Winter Wolpaw (Hrsg.), Brain-Computer Interfaces, Oxford 2012, S. 79-212.

Paal, Boris, 2021, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl.

Paal, Boris/Hennemann, Moritz, 2021, in: Paal, Boris P./Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl.

Pampaloni, Niccolò Paolo/Giugliano, Michele/Scaini, Denis/Ballerini, Laura/Rauti, Rossana: Advances in Nano Neuroscience: From Nanomaterials to Nanotools, Frontiers in Neuroscience 2019, S. 1-16.

Paszkiel, Szczepan/Rojek, Ryszard/Lei, Ningrong/Castro, Maria António: A Pilot Study of Game Design in the Unity Environment as an Example of the Use of Neurogaming on the Basis of Brain–Computer Interface Technology to Improve Concentration, NeuroSci 2021, S. 109-119.

Peksa, Janis/Mamchur, Dmytro: State-of-the-Art on Brain-Computer Interface Technology, Sensors 2023, S. 1-28.

Petri, Thomas, 2019, in: Smitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht DSGVO mit BDSG, 1. Aufl.

Petrlic, Ronald/Sorge, Christoph: Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Wiesbaden 2017.

Phillips, Elizabeth/Zhao, Xuan/Ullman, Daniel/Malle, Bertram F.: What is Human-like?: Decomposing Robots' Human-like Appearance Using the Anthropomorphic roBOT (ABOT) Database, HRI `18: Proceedings oft he 2018 ACM/IEEE International Conference on Human-Robot Interaction 2018, S. 105-113.

Pichiorri, Floriana/Morone, Giovanni/Petti, Manuela/Toppi, Jlenia/Pisotta, Iolanda/Molinari, Marco/Paolucci, Stefano/Inghilleri, Maurizio/Astolfi, Laura/Cincotti, Febo/Mattia, Donatella: Brain-computer interface boosts motor imagery practice during stroke recovery, Annals of Neurology 2015, S. 851-865.

Piltz, Carlo, 2018, in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl.

Pires, Gabriel/Torres, Mario/Casaleiro, Nuno/Nunes, Urbano/Castelo-Branco, Miguel: Playing Tetris with Non-Invasive BCI, Proceedings of the 2013 IEEE 2nd International Conference on Serious Games and Applications for Health 2011, S. 1-6.

Plath, Kai-Uwe, 2018, in: Plath, Kai-Uwe (Hrsg.): DSGVO BDSG, 3. Aufl.

Platon: Der Staat, Düsseldorf 2000. (Verlag: Artemis & Winkler)

Platon: Eutyphron, Göttingen 2014.

Pötters, Stephan, 2018, in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl.

Poullet, Yves/Dinant, Jean-Marc: Report On The Application Of Data Protection Principles To The Worldwide Telecommunication Networks, Strasburg 2004.

Pratt, Jay/Radulescu, Petre V./Guo, Ruo Mu/Abrams, Richard A.: It's Alive!: Animate Motion Captures Visual Attention, Psychological Science 2010, S. 1724-1730.

Przybylski, Andrew K./Murayama, Kou/DeHaan, Cody R./Gladwell, Valerie: Motivational, emotional, and behavioral correlates of fear of missing out, Computers in Human Behavior 2013, 1841–1848.

Qui, Qiong/Ruiz-Blondet, Maria V./Laszlo, Sarah/Jin, Zhanpeng: A Survey on Brain Biometrics, ACM Computing Surveys 2019, S. 1-38.

Quinn, Paul/Malgieri, Gianclaudio: The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework, German Law Journal 2021, S. 1583-1612.

Radbruch, Gustav: Rechtsphilosophie, 2. Aufl., Heidelberg 2003.

Rainey, Stephen/McGillivray, Kevin/Akintoye, Simi/Fothergill, Tyr/Bublitz, Christoph/Stahl, Bernd: Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?, Journal of Law and the Biosciences 2020, S. 1-19.

Rajaraman, Vaidyeswaran: Big Data Analytics, Resonance 2016, S. 695-716.

Rajendra, Gove Nitinkumar/Rajeneesh, Bedi Kaur: A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves, International Journal of Scientific and Engineering Research 2011, S. 1-4.

Ramírez-Moreno, Mauricio A./Carrillo-Tijerina, Patricio/Candela-Leal, Milton Osiel/Alanis-Espinosa, Myriam/Tudón-Martínez, Juan Carlos/Roman-Flores, Armando/Ramíret-Mendoza, Ricardo A./Lozoya-Santos, Jorge de J.: Evaluation of a Fast Test Based on Biometric Signals to Assess Mental Fatigue at the Workplace—A Pilot Study, International Journal of Enviromental Research and Public Health 2021, S. 1-20.

Rao, Rajesh P. N./Stocco, Andrea/Bryan, Matthew/Sarma, Devapratim, Youngquist/Wu, Joseph/Prat, Chantel S.: A Direct Brain-to-Brain Interface in Humans, PLOS ONE 2014, S. 1-12.

Rasmussen, Robert Gregory/Acharya, Soumyadipta/Thakor, N.v.: Accuracy of a Brain-Computer Interfaces in Subjects with Minimal Training, Proceedings of the IEEE 32nd Annual Northeast Bioengineering Conference 2006, S. 167-168.

Ravi, K. V. R./Palaniappan, Ramaswamy/Eswaran, C./Phon-Amnuaisuk, Somnuk: Data Encryption Using Event-releated Brain Signals, IEEE Conference on Computational Intelligence and Multimedia Applications 2007, S. 1-5.

Rawls, John: A Theory of Justice, Cambridge (USA) 1971.

Reck Miranda, Eduardo/Brouse, Andrew/Boskamp, Bram/Mullaney, Hilary: Plymouth Brain-Computer Music Interface Project: Intelligent Assistive Technology for Music-Making, Proceedings of International Computer Music Conference 2005, S. 1-4.

Reimer, Philipp, 2018, in: Sydow (Hrsg.), Gernot: Europäische Datenschutzgrundverordnung, 2. Aufl.

Reinsel, David/Gantz, John/Rydning, John: The Digitization of the World, 2018.

Reuderink, Boris/Nijholt, Anton/Poel, Mannes: Affective Pacman: A Frustrating Game for Brain-Computer Interface Experiments, in: Anton Nijholt/Dennis Reidsma/Hendri Hondorp (Hrsg.), Intelligent Technologies for Interactive Entertainment, Amsterdam 2009, S. 221-227.

Richter, Matthias/Kliner, Karin//Rennert, Dirk: Ergebnisse der BKK Umfrage „Digitalisierung, Arbeit und Gesundheit", in: Franz Knieps/Holger Pfaff (Hrsg.), Digitale Arbeit – Digitale Gesundheit, Berlin 2017, S. 107-124.

Richter, *Philipp:* Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 2015, S. 735-740.

Rocher, Luc/Hendrickx, Julien M./de Montojoye, Yves-Alexandre: Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications 2019, S. 1-9.

Rodrígues, Eva/Otero, Beatriz/Canal, Ramon: A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things, Sensors 2023, S. 1-24.

Ropohl, Günter: Allgemeine Technologie, 3. Aufl. Karlsruhe 2009.

Rosenfeld, Lisa/Torous, John/Vahia, Ipsit V.: Data Security and Privacy in Apss for Dementia: An Analysis of Existing Privacy Policies, The American Journal of Geriatric Psychiatry 2017, S. 873-877.

Roßnagel, Alexander, 2019., in: Smitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht DSGVO mit BDSG, 1. Aufl.

Roßnagel, Alexander/Nebel, Maxi/Richter, Philipp: Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, S. 455-460.

Roy, Raphaelle/Bonnet, Stéphane/Charbonnier, Sylvie/Campagne, Audrélie: Mental fatigue and working memory load estimation: Interaction and implications for EEG-based passive BCI, 35th Annual International Conference oft he IEEE EMBS 2013, S. 6607-6610.

Royer, Audrey/Doud, Alexander J./Rose, Minn L./He, Bin: EEG Control of a Virtual Helicopter in 3-Dimensinal Space Using Intelligent Control Strategies, IEEE Transactions on Neural Systems and Rehabilitation Engineering 2010, S. 581-589.

Rupp, Rüdiger/Kleih, Sonja C./Leeb, Robert/Millan, José del R./Kübler, Andrea/Müller-Putz, Gernot R.: Brain–Computer Interfaces and Assistive Technology, in: Gerd Grübler/Elisabeth Hildt (Hrsg.), Brain-Computer Interfaces in their ethical, social and cultural contexts, Dordrecht 2014, S. 7-38.

Safron, Adam/Klimaj, Victoria/Sylva, David/Rosenthal, A. M./Li, Meng/Walter, Martin/Bailey, J. Michael: Neural Correlates of Sexual Orientation in Heterosexual, Bisexual, and Homosexual Woman, Scientific Reports 2018 (8), S. 1-14.

Saha, Simanto/Mamun, Khondaker A./Ahmed, Khawza/Mostafa, Raqibul/Naik, Ganesh R./Darvishi, Sam/Khandoker, Ahsan H./Baumert, Mathias: Progress in Brain Computer Interface: Challenges and Opportunities, Frontiers in Systems Neuroscience 2021, S. 1-20.

Salahuddin, Usman/Gao, Pu-Xian: Signal Generation, Acquisition, and Processing in Brain Machine Interfaces: A Unified Review, Frontiers in Neuroscience 2021, S. 1-21.

Samhita, Laasya/Gross, Hans J.: The „Clever Hans Phenomenon" revisited, Communicative & Integrative Biology 2013, S. 1-3.

Sanna, Andrea/Manuri, Federico/Fiorenza, Jacopo/De Pace, Francesco: BARI: An Affordable Brain-Augmented Reality Interface to Support Human–Robot Collaboration in Assembly Tasks, Information 2022, S. 1-14.

Santamaría-Vázquez, Eduardo/Martínez-Cagigal, Víctor/Marcos-Martínez, Diego/Rodríguez-González, Víctor/Pérez-Velasco, Sergio/Moreno-Calderón, Selene: MEDUSA©: A novel Python-based software ecosystem to accelerate brain-computer interface and cognitive neuroscience research, Computer Methods and Programs in Biomedicine 2023, S. 1-9.

Schaar, Katrin: DS-GVO: Geänderte Vorgaben für die Wissenschaft, ZD 2016, S. 224-226.

Schantz, Peter, 2017, in: Schantz, Peter/Wolff, Heinrich Amadeus (Hrsg.): Das neue Datenschutzrecht,

Schantz, Peter, 2019, in: Smitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht DSGVO mit BDSG, 1. Aufl.

Schantz, Peter, 2020, in: Wolff, Heinrich Amadeus/ Brink, Stefan (Hrsg.), Stefan: BeckOK Datenschutzrecht, 36. Aufl.

Schefzig, Jens: Big Data = Personal Data? Der Personenbezug von Daten bei Big Data-Analysen, DSRITB 2014, S. 103-119.

Schiff, Alexander, 2018, in: in: Ehmann, Eugen/ Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung DS-GVO.2. Aufl.

Schild, Hans Hermann, 2020, in: Wolff, Heinrich Amadeus/ Brink, Stefan (Hrsg.), Stefan: BeckOK Datenschutzrecht, 36. Aufl.

Schmidt, Ingrid, 2021, in: Müller-Glög/Preis/Schmidt (Hrsg.): ErfK zum Arbeitsrecht, 21. Aufl.

Schmidt-Wudy, Florian, 2020, in: Wolff, Heinrich Amadeus/ Brink, Stefan (Hrsg.), Stefan: BeckOK Datenschutzrecht, 36. Aufl.

Schneider, Frank/Fink, Gereon R.: Einführung, in: Frank Schneider/ Gereon R. Fink (Hrsg.), Funktionelle MRT in Psychiatrie und Neurologie, 2. Aufl., 2013, S. 1-4.

Schneider, Jana/Schindler, *Stephan:* Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten, ZD 2018, S. 463-469.

Schneider, Jochen: Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, S. 303-307.

Schreiber, Darren/Fonzo, Greg/Simmons, Alan N./Dawes, Christopher T./Flagan, Taru/ Fowler, James H./Paulus, Martin P.: Red Brain, Blue Brain: Evaluative Processes Differ in Democrats and Republicans, PLOS ONE 2013, S. 1-6.

Schultze-Melling, Jyn, 2022, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG, 4. Aufl.

Schulz, Sebastian, 2018, in: Gola, Peter (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl.

Schulz, Sebastian: Privacy by Design, CR 2012, S. 204-208.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.): DS-GVO/BDSG, Kommentar, Heidelberg 2018.

Schwarz, Christopher G./Kremers, Walter K./Therneau, Terry M./Sharp, Richard R./ Gunter, Jeffery L./Vemuri, Prashanthi/Arani, Arvin/Spychella, Anthony J./Kantarci, Kejal/Knopman, David S./Petersen, Ronald C./Jack Jr., Clifford R.: Identification of Anonymous MRI Research Perticipants with Face-Recognition Software, The New England Journal of Medicine 2019, S. 1684-1686.

Schwemmer, Michael A./Skomrock, Nicholas D./Sederberg, Per B./Ting, Jordyn E./Sharma, Gaurav/Bockbrader, Marcia A./Friedenberg, David A.: Meeting brain-computer interface user performance expectations using a deep neural network decoding framwork, nature medicine 2018, S. 1669-1679.

Sebastián-Romagosa, Marc/Cho, Woosang/Ortner, Rupert/Murovec, Nensi/Von Oertzen, Tim/Kamada, Kyousuke/Allison, Brendan Z./Guger, Christoph: Brain Computer Interface Treatment for Motor Rehabilitation of Upper Extremity of Stroke Patients – A Feasibility Study, Frontiers of Neuroscience 2020, S. 1-12.

Shah, Uzair/Alzubaidi, Mahmood/Mohsen, Farida/Abd-Alrazaq, Alaa/Alam, Tanvir/Househ, Mowafa: The Role of Artificial Intelligence in Decoding Speech from EEG Signals: A Scoping Review, Sensors 2022, S. 1-15.

Shan, Hongchang/Liu, Yu/Stefanov, Todor: A Simple Convolutional Neural Network for Accurate P300 Detection and Character Spelling in Brain Computer Interface, Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence 2018, S. 1604-1610.

Shih, Jerry J./Krusienski, Dean J./Wolpaw, Jonathan R.: Brain-Computer Interfaces in Medicine, Mayo Clinic Proceedings 2012, S. 268-279.

Smalley, Eric: The business of brain-computer interfaces, Nature Biotechnology 2019, S. 978-982.

Soekadar, Surjo R./Nann, Marius/Crea, Simona/Trigili, Emilio/Gómez, Cristina/Opisso, Eloy/Cohen, Leonardo G./Birbaumer, Niels/Vitiello, Nicola: Restoration of Finger and Arm Movements Using Hybrid Brain/Neural Assistive Technology in Everyday Life Environments, in: Christoph Guger/Brendan Z. Allison/Natalie Mrachacz-Kersting (Hrsg.), Brain-Computer Interface Research, Cham 2019, S. 53-62.

Soori, Mohsen/Arezoo, Behrooz/Dastres, Roza: Internet of things for smart factories in industry 4.0, a review, Internet of Things and Cyber-Physical Systems 2023, S. 192-204.

Specht, Louisa, 2018, in: Sydow (Hrsg.), Gernot: Europäische Datenschutzgrundverordnung, 2. Aufl.

Spiekermann, Markus: Chancen und Herausforderungen in der Datenökonomie, Aus Politik und Zeitgeschichte 2019, S. 16-21.

Spindler, Gerald/Dalby, Lukas, 2019, in: Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 4. Aufl.

Spindler, Gerald/Horváth, Anna Zsófia, 2019, in: Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 4. Aufl.

Spindler, Gerald: Big Data und Forschung mit Gesundheitsdaten in der gesetzlichen Krankenversicherung, Medizinrecht 2016, S. 691-699.

Srijony, Tashnova Hasan/Rashid, Khalid Hasan Ur/Chakraborty, Utchash/Badsha, Imran/Morol, Kishor: A Proposed Home Automation System for Disable People Using BCI System, Proceedings of International Joint Conference on Advances in Computational Intelligence 2021, S. 1-15.

Stammler, Rudolf: Lehrbuch der Rechtsphilosophie, 2. Aufl., Berlin 1923.

Stawicki, Piotr/Gembler, Felix/Volosyak, Ivan: Driving a Semiautonomous Mobile Robotic Car Controlled by an SSVEP-Based BCI, Computational Intelligence and Neuro-science 2016, S. 1-14.

Steinfeld, Nili: „I agree tot he terms and conditions": (how) do users read privacy policies online? An eye-tracking experiment, Computers in Human Behavior 2016, S. 992-1000.

Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider: Grundfragen des Datenschutzes, BT-Drucksache VI/3826, Bonn 1971.

Sterman, Maurice/Friar, Linda: Suppression of seizures in an epileptic following sensorimotor EEG feedback training, Electroencephalography and Clincal Neurophysiology 1972, S. 89-95.

Stollhoff, Susanne, 2020, in: Eßer, Martin/Kramer, Philipp/von Lewinski, Kai (Hrsg.): DSGVO BDSG, 7. Aufl.

Straebel, Volker/Thoben, Wilm: Alvin Lucier's Music for Solo Performer: Experimental music beyond sonification, Organised Sound 2014, S. 17-29.

Strahilevitz, Lior/Kugler, Matthew B.: Is Privac Policy Language Irrelevant to Consumers?, Coase-Sandor Working Paper Series in Law and Economics 2016, S. 1-28.

Tabassum, Madiha/Alqhatani, Abdulmajeed/Aldossari, Marran/Richter Lipford, Heather: Increasing User Attention with a Comic-based Policy, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems 2018, S. 1-6.

Taeger, Jürgen, 2019, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG, 3. Aufl.

Taeger, Jürgen, 2022, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG, 4. Aufl.

Takabi, Hassan: Firewall for Brain: Towards a Privacy Preserving Ecosystem for BCI Applications, IEEE Conference on Communications and Network Security 2016, S. 1-2.

Tang, Xin/Shen, Hao/Zhao, Siyuan/Li, Na/Liu, Jia: Flexible brain–computer interfaces, Nature Electronics 2023, S. 109-118.

Tang, Yuchun/Hojatkashain, Cornelius/Dinov, Ivo/Sun, Bo/Fan, Lingzhong/Lin, Xiangtao/Qi, Hengtao/Hua, Xue/Liu, Shuwei/Toga, Arthur W.: The construction of a Chinese MRI brain atlas: A morphometric comparison study between Chinese and Caucasian cohorts, NeuroImage 2010, S. 33-41.

Tangermann, Michael/Krauledat, Matthias/Grzeska, Konrad/Sagebaum, Max/Blankertz, Benjamin/Vidaurre, Carmen/Müller, Klaus-Robert: Playing Pinball with non-invasive BCI, Advances in Neural Information Processing Systems 2008, S. 1641-1648.

Teismann, Tobias/ Brailovskaia, Julia/Schaumburg, Svenja/Wannemüller, André: High place phenomenin: prevalence and clinical correlates in two German samples, BMC Psychiatry 2020, S. 1-7.

Teo, Sze-Hui Jane/Poh, Xue Wie Wendy/Lee, Tih Shih/Guan, Cuntai/Cheung, Yin Bun/Fung, Daniel Shuen Sheng/Zhang, Hai Hong/Chin, Zheng Yang/Wang, Chuan Chu/Sung, Min/Goh, Tze Jui/Wenig, Shih Jen/Tng, Xin Jie Jordon/Lim, Choon Guan: Brain-computer interface based attention and social cognition training programme for children with ASD and co-occurring ADHD: A feasibility trial, Research in Autism Spectrum Disorders 2021, S. 1-14.

Tonin, Luca/Carlos, Tom/Leeb, Robert/del R Millán, José: Brain-controlled telepresence robot by motor-disabled people, Proceedings of the annual international conference of the IEEE EMBS 2011, S. 1-4.

Torre, Damiano/Abualhaija, Sallam/Sabetzadeh, Mehrdad/Briand, Lionel/Baetens, Katrien/Goes, Peter/Forastier, Sylvie: An AI-assisted Approach for Checking the Completeness of Privacy Policies Against GDPR, IEEE 28th International Requirements Engineering Conference (RE) 2020, S. 136-146.

Tuchel, Klaus: Herausforderung der Technik, Bremen 1967.

Tudour, Mario/Tudor, Lorainne/Tudor, Katarina Ivana: Hans Berger (1873-1941) - The history of electroencephalography, Acta medica Croatica 2005, S. 307-313;

Ullah, Amin/Anwar, Syed Myhammad/Li, Jianqiang/Nadeem, Lubna/Mahmood, Tariq/Rehman, Amjad/Saba, Tanzila: Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment, Complex & Intelligent Systems 2024, S. 1607-1637.

van de Laar, Bram/Gürkök, Hayrettin/Plass-Oude Bos, Danny/Poel, Mannes/Nijholt, Anton: Experiencing BCI Control in a Popular Computer Game, IEEE Transactions on Computational Intelligence and AI in Games 2013, S. 176-184.

van Erp, Jan B.F./Lotte, Fabien/Tangermann, Michael: Brain-Computer Interfaces: Beyond Medical Applications, Computer 2012, S. 26-34.

Vargas Martin, Miguel/Cho, Victor/Aversano, Gabriel: Detection of Subconscious Face Recognition Using Consumer-Grade Brain-Computer Interfaces, ACM Transactions on Applied Perception 2016, Article 7 S. 1-20.

Vasa, Jalpesh/Thakkar, Amit: Deep Learning: Differential Privacy Preservation in the Era of Big Data, Journal of Computer Information Systems 2023, S. 608-631.

Vecchiato, Giovanni/Astolfi, Laura/De Vico Fallani, Fabrizio/Dalinari, Serenella/Cincotti, Febo/Aloise, Fabio/Mattia, Donatella/Marciani, Maria Grazia/Bianchi, Luigi/Soranzo, Ramon/Babiloni, Fabio: The study of brain activity during the observation of commericals advertising by using high resolution EEG techniques, et al., 31st Annual International Conference oft he IEEE EMBS 2009, S. 57-60.

Veil, Winfried: DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip Eine erste Bestandsaufnahme, ZD 2015, S. 347-353.

Vidal, Jacques: Toward Direct Brain-Computer Communication, Annual Review of Biophysics and Bioengineering 1973, S. 157-180.

Vinothraj, Thangarajah/Alfred, Denshiya Dominic/Amarakeerthi, Senaka/Ekanayake, Jayalath B.: BCI-Based Alcohol Patient Detection, et al., Conference Papers IFSA-SCIS 2017, S. 1-6.

Voigt, Marlene: Die datenschutzrechtliche Einwilligung, Baden-Baden 2020.

Voigt, Paul, 2019, in: Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO – BDSG, 3. Aufl.

Voigt, Paul/von dem Bussche, Axel: EU-Datenschutz-Grundverordnung (DSGVO), Berlin 2018.

von Aquin, Thomas: Summa Theologiae II-II, 2. Aufl., London 1920.

Voß, Jakob: Was sind eigentlich Daten?, LIBREAS 2013, S. 4-11.

Vossenkuhl, Cosima: Der Schutz genetischer Daten, München 2013.

Wahlstrom, Kirsten/Fairweather, Ben/Ashman, Helen: Brain-computer interfaces: A technical approach to supporting privacy, Proceedings of the. 12th Int. Ethicomp Conference 2011, S. 471-479.

Wang, Jing/Cherkassky, Vladimir L./Just, Marcel Adam: Predicting the Brain Activation Pattern Associated With the Propositional Content of a Sentence: Modeling Neural Representations of Events and States, Human Brain Mapping 2017, S. 4865-4881.

Wang, Ker-Jiun/Zhen, Caroline Yan/Shidjaman, Mohammad/Wairagkar, Maitreyee/von Mohr, Mariana: Jean Joseph v2.0 (REmotion): Make Remote Emotion Touchable, Seeable and Thinkable by Direct Brain-toBrain Telepathy Neurohaptic Interface Empowered by Generative Adversarial Network, IEEE International Conference on SMC 2020, S. 3488-3493.

Wang, Yijun/Jung, Tzyy-Ping: A Collaborative Brain-Computer Interface for Improving Human Performance, PLOS ONE 2011, S. 1-11.

Warner, Mark R./Fisher, Deb: Deceptive Experiences To Online Users Reduction (DETOUR) Act, 2019.

Weber, Max: Wirtschaft und Gesellschaft, 5. Aufl., Tübingen 1921.

Wedde, Peter, 2020, in: Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke (Hrsg.): EU-DSGVO und BDSG.

Weichert, Thilo, 2020, in: Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung/BDSG, 3. Aufl.

Weinzierl, Quirin: Dark Patterns als Herausforderung für das Recht, NvWZ 2020, S. 1-11.

Westin, Alan F.: Privacy and Freedom, New York 1967.

Williams, Lisa A./Brosnan, Sarah F./Clay, Zanna: Anthropomorphism in comparative affective science: Advocating a mindful approach, Neuroscience & Biobehavioral Reviews 2020, S. 299-307.

Wolff, Heinrich Amadeus, 2017, in: Schantz, Peter/Wolff, Heinrich Amadeus (Hrsg.): Das neue Datenschutzrecht,

Wolpaw, Jonathan R./Winter Wolpaw, Elizabeth: Brain-Computer Interfac-es: Something new under the sun, in: Jonathan R. Wolpaw/Elizabeth Winter Wolpaw (Hrsg.), Brain-Computer Interfaces, Oxford 2012, S. 3-12.

Wong, Rebecca: Data Protection Online: Alternative Approaches to Sensitive Data?, Journal of International Commercial Law and Technology 2007, S. 9-16.

Woyke, Andreas: Human Enhancement und seine Bewertung – eine kleine Skizze, In: Andreas Woyke/Reinhard Heil/Stefan Gammel/Christopher Coenen (Hrsg.), Die Debatte über »Human Enhancement«, Bielefeld 2010, S. 21-38.

Xu, Baoguo/Li, Wenlong/He, Xiaohang/Wie, Zhiwei/Zhang, Dalin/Wu, Changcheng/Song, Aiguo: Motor Imagery Based Continuous Teleoperation Robot Control with Tactile Feedback, Electronics 2020 S. 1-16.

Xu, Baoguo/Li, Wenlong/Liu, Deping/Zhang, Kun/Miao, Minmin/Xu, Gouzheng/Song, Aiguo: Continuous Hybrid BCI Control for Robotic Arm Using Noninvasive Electroencephalogram, Computer Vision, and Eye Tracking, Mathematics 2022, S. 1-20.

Yanagisawa, Takufumi/Hirata, Masayuki/Saitoh, Youichi/Kishima, Haruhiko/Matsushita, Kojiro/Goto, Tetsu/Fukuma, Ryohei/Yokoi, Hiroshi/Kamitani, Yukiyasu/Yoshimine, Toshiki: Electrocorticographic Control of aProsthetic Arm in Paralyzed Patients, Annals of Neurology 2012, S. 353-361.

Yanagisawa, Takufumi/Hirata, Masayuki/Saitoh, Youichi/Kishima, Haruhiko/Matsushita, Kojiro/Goto, Tetsu/Fukuma, Ryohei/Yokoi, Hiroshi/Kamitani, Yukiyasu/Yoshimine, Toshiki: Electrocorticographic Control of aProsthetic Arm in Paralyzed Patients, Annals of Neurology 2012, S. 353-361.

Youyuo, Wu/Kosinski, Michal/Stillwell, David: Computer-based personality judgments are more accurate than those made by humans, PNAS 2014, S. 1036-1040.

Zhang, Biao/Wang, Jianjun/Fuhlbrigge, Thomas: A Review oft he Commercial Brain-Computer Interface Technology from Perspective of Industrial Robotics, Proceedings of the 2010 IEEE 2010, S. 379-384.

Zhang, Meng/Raghunathan, Anand/Jha, Niraj K.: MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection, IEEE Transactions on Biomedical Circuits and Systems 2013, S. 871-881.

Zhao, Zhi-Ping/Nie, Chuang/Jiang, Cheng-Teng/Cao, Sheng-Hao/Tian, Kai-Xi/Yu, Shan/Gu, Jian-Wen: Modulating Brain Activity with Invasive Brain–Computer Interface: A Narrative Review, Brain Sciences 2023, S. 1-14.

Zuboff, Shoshana: Aus Politik und Zeitgeschichte 2019, S. 4-9.

Zuiderveen Borgesius, Frederik J./Möller, Judith/Kruikemeier, Sanne/Ó Fathaigh, Ronan/Irion, Kristian/Dobber, Tom/Bodo, Balazs/de Vreese, Claes: Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018, S. 82-96.

Zuse, Horst: Der lange Weg zum Computer: Von Leibnitz' Dyadik zu Zuses Z3, in: Martin Grötschel/Eberhard Knobloch/Juliane Schiffers/Mimmi Woisnitza/Günther M. Ziegler (Hrsg.), Vision als Aufgabe – das Leibnitz Universum im 21. Jahrhundert, Berlin 2016, S. 111-124.

Web

Angwin, Julia/Varner, Madeleine/Tobin, Ariana: Facebook Enabled Advertisers to Reach „Jew Haters", v. 14.9.2017, https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2024, v. 12.11.2024, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5.

Bundeskriminalamt, Bundeslagebild Cybercrime 2023, v. 13.5.2024, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=28110.

Cass, Stephen: The Tech Behind the Mind-Reading Pangolin Dress Could Lead to Wireless - and Batteryless - Exoskeleton Control, v. 11.9.2020, https://spectrum.ieee.org/the-tech-behind-a-mind-reading-dress-could-lead-to-wireless-batteryless-exoskeleton-control.

Chudler, Eric H./Johnson, Lise: Brain-Computer Interfaces and the Future of Humanity, v. 23.4.2017, https://www.psychologytoday.com/us/blog/brain-bytes/201704/brain-computer-interfaces-and-the-future-humanity.

Constine, Josch: Facebook is building brain-computer interfaces for typing and skin-hearing, v. 19.4.2017, https://tcrn.ch/2Y7iALc

Drew, Liam: Elon Musk's Neuralink brain chip: what scientist think of first human trial, v. 2.2.2024, https://www.binasss.sa.cr/bibliotecas/bhm/feb24/34.pdf.

Gera, Emily: The Neuroscience of Mind-Control Gaming, v. 26.11.2018, https://variety.com/2018/gaming/features/brain-computer-interface-neurable-1203036143/.

Hagey, Keach/Horwitz, Jeff: Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead., v. 15.9.2021, https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215#refreshed?mod=article_inline.

Konstadinov, Dimitar: Hacking Implantable Medical Devices, v. 28.4.2014, https://resources.infosecinstitute.com/topic/hcking-implantable-medical-devices/.

Moerel, Lokke/Prins, Corien: 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.

Musk, Elon/Neuralink: An Integrated Brain-Machine Interface Platform with Thousands of Channels, v. 16.7.2019, https://www.biorxiv.org/content/10.1101/703801v4.full.pdf.

Purnell, Newley/Horwitz, Jeff: Facebook Services Are Used to Spread Religios Hatred in India, Internal Documents Show, v. 23.10.2021, https://www.wsj.com/articles/facebook-services-are-used-to-spread-religious-hatred-in-india-internal-documents-show-11635016354?mod=article_inline.

Ruffio, Patricia: Dark Web Price Index 2022, v. 19.9.2022, https://www.privacyaffairs.com/dark-web-price-index-2022/.

Wells, Georgia/Seetharaman, Deepa/Horwitz, Jeff: Is Facebook Bad for You? It Is for About 350 Million Users, Company Survery Suggest, v. 5.11.2021, https://www.wsj.com/articles/facebook-bad-for-you-360-million-users-say-yes-company-documents-facebook-files-11636124681#refreshed?mod=article_inline.

Wong, Julia Carrie: It might work too well": the dark art of political advertising online, v. 19.3.2018, https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy.

Zhang, Qiqi/Liu, Ying: Improving brain computer interface performance by data augmentation with conditional Deep Convolutional Generative Adversial Networks, v. 19.6.2018, https://arxiv.org/abs/1806.07108.