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.