K. Grundsätze der Verarbeitung

I. Analyse von Art. 5 DSGVO

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

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

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

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

a. Rechtmäßigkeit

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

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

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

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

b. Verarbeitung nach Treu und Glauben

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

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

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

c. Transparenz

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

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

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

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

a. Rechtmäßigkeit bei der Verarbeitung von Wesensdaten

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

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

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

b. Treu und Glauben bei der Verarbeitung von Wesensdaten

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

c. Transparenz bei der Verarbeitung von Wesensdaten

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Zweckbindung bei der Verarbeitung von Wesensdaten

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

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

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

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

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

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

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

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

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

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

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

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

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

6. Datenminimierung bei der Verarbeitung von Wesensdaten

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

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

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

7. Art. 5 Abs. 1 lit. d DSGVO: Richtigkeit

Bereits das BVerfG hatte in seinem wegweisenden Volkszählungsurteil aus dem Jahre 1983 darauf hingewiesen, dass durch die digitale Datenverarbeitung umfassende Persönlichkeitsprofile erstellt werden können, über die betroffene Personen keinerlei Kontrolle bzgl. Richtigkeit und Verwendung der Daten mehr haben.[763] Im gleichen Verständnis fordert Art. 5 Abs. 1 lit. d DSGVO, dass personenbezogene Daten sachlich richtig sowie erforderlichenfalls auf dem neuesten Stand sein müssen und, dass angemessene Maßnahmen ergriffen werden müssen, um personenbezogene Daten, die in Bezug auf den zugrundeliegenden Zweck unrichtig sind, unverzüglich zu löschen oder zu berichtigen.

Sachlich richtig sind personenbezogene Daten dann, wenn diese nach objektiver Einschätzung der Realität entsprechen.[764] Nur so kann gewährleistet werden, dass Sachverhalte und Situationen, die die betroffene Person betreffen, wahrheitsgemäß auf Grundlage der Daten rekonstruiert werden können.[765] Diese Voraussetzung betrifft dabei nicht nur Tatsachenangaben, sondern auch Werteurteile, wenn diese bspw. auf falschen Tatsachen beruhen oder von falschen Prämissen ausgehen.[766]

Während die sachliche Richtigkeit grundsätzlich zu beachten ist, müssen personenbezogene Daten lediglich „erforderlichenfalls" auf dem neusten Stand sein.[767] Wenn der Verarbeitungszweck eine Verarbeitung von historischen Daten notwendig macht, z.B. wenn in einer Patientenakte noch Ge-

763 BVerfG, Urt. v. 15.12.1983 - 1 BvR 209/83, NJW 1984, 421.
764 *Herbst* (2020), Art. 5 Rn. 60.
765 *Frenzel* (2021) BDSG, Art. 5 Rn. 39.
766 *Schantz* (2020), Art. 5 Rn. 27; anderer Meinung: *Herbst* (2020), Art. 5 Rn. 60; *Roßnagel* (2019), Art. 5 Rn. 140.
767 *Voigt* (2019), Art. 5 Rn. 31.

sundheitszustände festgehalten sind, die zwar zum jetzigen Zeitpunkt nicht mehr die Realität abbilden, aber eine Entwicklung dokumentieren, dann müssen die Daten nicht nur dem neusten Stand angepasst werden.[768] Ob eine Anpassung der Daten an dem neusten Stand tatsächlich erforderlich ist, ist daran zu bemessen, inwiefern unrichtige Daten schädlich für den Verarbeitungszweck und damit auch für die betroffenen Personen sind.[769] Dies trifft meistens dann zu, wenn die Aktualität der personenbezogenen Daten wesentlich für den Verarbeitungszweck ist. So ist es bspw. bei der Prüfung einer möglichen Kreditvergabe zwingend notwendig, dass Daten zum Vermögen, zum Einkommen und zu bestehenden Schulden auf dem neusten Stand sind, damit eine faire Kreditvergabe vorgenommen werden kann.

Art. 5 Abs. 1 lit. d Hs. 2 DSGVO ergänzt diese Kriterien um die Notwendigkeit, unrichtige Daten unverzüglich zu berichtigen oder zu löschen. Daraus geht hervor, dass der Verantwortliche angemessene Maßnahmen ergreifen muss, um die Richtigkeit der personenbezogenen Daten kontinuierlich und aktiv zu überprüfen.[770] Eine solche Maßnahme könnte kontextbedingt z.B. eine regelmäßige Kontrolle des Datenbestands[771] bzw. dessen Abgleich mit Angaben der betroffenen Personen sein. Erweitert wird dieses Merkmal um das Recht der betroffenen Person auf Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) und Einschränkung der Verarbeitung (Art. 18 DSGVO).

Die Richtigkeit der Daten spielt besonders dann eine Rolle, wenn die betroffene Person auf Grundlage der personenbezogenen Daten Rechtsfolgen zu befürchten hat.[772] In diesem Zuge sind vor allem Profiling-Maßnahmen erwähnenswert, die ggf. große Auswirkungen für die Rechte und Freiheiten der betroffenen Person haben könnten.[773] Aus diesem Grund konkretisiert ErwG. 71 S. 6 auch, dass beim Profiling geeignete technische und organisatorische Maßnahmen getroffen werden müssen, die ausreichend sicherstellen, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird. Auch bei KI ist dahingehend zu berücksichtigen, dass geeignete Trainings-

768 *Roßnagel* (2019), Art. 5 Rn. 141; *Herbst* (2020), Art. 5 Rn. 61; *Voigt* (2019), Art. 5 Rn. 31.
769 *Reimer* (2018), Art. 5 Rn. 36; *Herbst* (2020), Art. 5 Rn. 62.
770 *Pötters* (2018), Art. 5 Rn. 24.
771 *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 13.
772 *Frenzel* (2021) BDSG, Art. 5 Rn. 39.
773 *Art.-29-Gruppe,* WP 251 1 rev. 01, 2017, S. 11.

daten verwendet werden, damit die KI nicht falsche oder diskriminierende Ergebnisse/Daten erzeugt.[774]

8. Richtigkeit bei der Verarbeitung von Wesensdaten

Im Zuge der Betrachtung der Einwilligung mittels BCI wurde bereits festgestellt, dass die Übersetzung der Gehirnaktivitäten in entsprechende Outputs ein Problem darstellen könnten, wenn diese nicht korrekt ist. Dieser Aspekt ist auch bei der Einhaltung des Grundsatzes der Richtigkeit relevant. Verantwortliche müssen demnach sicherstellen, dass die relevanten Signale korrekt aufgezeichnet werden sowie, dass die zugrundeliegende Software lediglich richtige Urteile trifft, die den zugrundeliegenden Signalen entsprechen.

Diese Maßgabe überträgt sich auch auf die notwendige Aktualität der Daten. Während die neurologischen Signale logischerweise zu jeder Zeit aktuell sind, da diese in Echtzeit direkt aus dem Gehirn der Nutzer ausgelesen werden, muss dies für die Übersetzung nicht gelten. Es ist bspw. denkbar, dass neue Erkenntnisse zu Gehirnaktivitäten dazu führen, dass auch die Übersetzung angepasst werden muss. Der Verantwortliche muss demnach kontinuierlich sicherstellen, dass die eingesetzten Systeme neue Informationen berücksichtigen, damit die Übersetzung zu jeder Zeit aktuell ist. Insbesondere bedeutet dies, dass die Richtigkeit bei den Trainingsdaten des Übersetzungsalgorithmus gewährleistet werden muss. Diese kontinuierliche Überprüfung würde ebenso sicherstellen, dass keine unrichtigen Daten mehr verarbeitet werden würden.

9. Art. 5 Abs. 1 lit. e DSGVO: Speicherbegrenzung

Um eine zeitlich unbegrenzte Speicherung von personenbezogenen Daten zu verhindern, fordert die DSGVO, dass die Möglichkeit der Identifizierung einer betroffenen Person nur so lange durch die Daten ermöglicht werden darf, wie es für den zugrundeliegenden Zweck notwendig ist. Damit ergänzt der Gesetzgeber die Zweckbindung um eine zeitliche Komponente.[775] Durch ErwG. 39 S. 8 wird konkretisiert, dass sich die Speicherfrist

774 *Schantz* (2020), Art. 5 Rn. 27.
775 *Pötters* (2018), Art. 5 Rn. 25; *Herbst* (2020), Art. 5 Rn. 65.

an dem unbedingt erforderlichen zeitlichen Mindestmaß zu orientieren hat. Der Begriff „Speichern" beschreibt dabei das technische Vorhalten von Daten, um diese weiter zu verarbeiten oder zu nutzen.[776]

Dabei gibt es verschiedene Möglichkeiten, dieser Verpflichtung der Speicherbegrenzung nachzukommen. Naheliegend ist die Löschung der Daten vom entsprechenden Datenträger, sodass diese nicht mehr aufrufbar sind und somit auch keine Identifikation von Betroffenen mehr möglich ist.[777] Gleiches kann auch erreicht werden, wenn die relevanten Datenträger ausreichend zerstört werden.[778] Abschließend geht aus der konkreten Formulierung des Gesetzestexts noch eine andere Möglichkeit hervor. Art. 5 Abs. 1 lit. e DSGVO stellt nämlich nicht auf die Speicherung als solche ab, sondern auf die Möglichkeit der Identifizierung der betroffenen Person.[779] Demnach ist eine Speicherbegrenzung auch mit einer Anonymisierung der personenbezogenen Daten denkabr, womit die Identifikation der Betroffenen nicht mehr möglich wäre.[780]

Damit Verantwortliche sich auch tatsächlich an diese Vorgaben halten, sieht ErwG. 39 S. 10 vor, dass dieser Fristen für die Löschung oder die regelmäßige dahingehende Überprüfung von personenbezogenen Daten festlegt. Sinnvoller ist es allerdings, die Fristsetzung nicht alternativ zur Überprüfung zu sehen und vice versa, sondern diese Maßnahmen als gegenseitige Ergänzung zu verstehen.[781] Ein Verantwortlicher muss somit genau wissen, welche Datenarten verarbeitet werden und welche gesetzlichen Aufbewahrungs- und Löschpflichten bestehen, damit diese mit den eigenen Aufbewahrungsinteressen abgeglichen werden können, um dann konkrete Aufbewahrungs- und Löschfristen für die jeweiligen Datenarten festzulegen, anhand derer eine kontrollierte Löschung garantiert werden kann.[782] Dieser Prozess sollte zusätzlich regelmäßig auf Aktualität und Angemessenheit überprüft werden.

Wie bei der Zweckbindung gemäß Art. Art. Abs. 1 lit. b DSGVO besteht eine Ausnahme von der Speicherbegrenzung, wenn personenbezogene Daten ausschließlich für im öffentlichen Interesse liegende Archivzwecke, für

776 *Roßnagel* (2019), Art. 4 Rn. 19.
777 *Herbst* (2020), Art. 5 Rn. 66.
778 *Reimer* (2018), Art. 5 Rn. 40.
779 *Roßnagel* (2019), Art. 5 Rn. 155.
780 *Herbst* (2020), Art. 5 Rn. 66; *Roßnagel* (2019), Art. 5 Rn. 155; *Reimer* (2018), Art. 5 Rn. 40.
781 *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 14.
782 *Voigt* (2019), Art. 5 Rn. 36.

wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 DSGVO verarbeitet werden.

10. Speicherbegrenzung bei Verarbeitung von Wesensdaten

Mit der Notwendigkeit der Speicherbegrenzung entsteht ein Spannungsverhältnis beim Einsatz von BCI. Grundsätzlich würde sich die Speicherdauer der verarbeiteten Wesensdaten nach Art. 17 Abs. 1 DSGVO richten, womit die Daten dann gelöscht werden müssten, sobald der Zweck der Verarbeitung erreicht wurde. Bei einer strengen Auslegung würde dies bedeuten, dass die neurologischen Signale und die darauf aufbauenden Übersetzungen dann gelöscht werden müssen, sobald der gewünschte Output erzeugt wurde. Bei einer etwas gemäßigteren Auslegung könnten die Daten noch für eine gewisse Dauer vorgehalten werden, z.B. für einen Monat oder bis die Person die Technologie nicht mehr nutzt oder ihre Einwilligung zurückzieht. Wie allerdings bei der Betrachtung der Richtigkeit der Daten festgestellt wurde, ist der Verantwortliche auch dazu verpflichtet, die Trainingsdaten und die daraus resultierenden Übersetzungen aktuell und korrekt zu halten. Dieser Pflicht kann nur nachgekommen werden, wenn die Daten langfristig gespeichert werden dürfen. Diesem Spannungsverhältnis kann der Verantwortliche allerdings damit entkommen, indem dieser bereits vor Beginn der Verarbeitung bspw. die Einwilligung für den Zweck einholt, dass die erhobenen Wesensdaten auch für die notwendige Optimierung des Systems verwendet werden dürfen. Eine andere Möglichkeit wäre eine Weiterverarbeitung auf Grundlage von Art. 5 Abs. 1 lit. b DSGVO. Das Training des Systems kann als KI-Forschung angesehen werden, womit ein wissenschaftlicher Forschungszweck vorliegen würde.

11. Art. 5 Abs. 1 lit. f DSGVO: Integrität und Vertraulichkeit

Gemäß dem Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. f DSGVO, muss bei der Datenverarbeitung ein angemessener Schutz der personenbezogenen Daten vorliegen. Dieser Schutz soll durch geeignete technische und organisatorische Maßnahmen gewährleistet werden und einschließlich vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung schützen. Die Aufzählung ist dabei nicht abschließend,

sondern nur exemplarisch[783] und macht deutlich, dass eine umfassende IT-Sicherheit gefordert wird.[784] Der Teilaspekt der unbefugten Verarbeitung adressiert dabei vor allem den Zugang zu sowie die Verarbeitung von personenbezogenen Daten durch unbefugte Dritte und der Teilaspekt der unrechtmäßigen Verarbeitung umfasst den Fall, wenn personenbezogene Daten vom Verantwortlichen ohne ausreichende Rechtsgrundlage verarbeitet werden.[785] Auch ErwG. 39 S. 12 stellt nochmal besonders auf die Sicherheit und Vertraulichkeit ab und unterstreicht die Tatsache, dass Unbefugte keinen Zugang zu Daten haben und diese auch nicht verarbeiten sollten. Die Teilaspekte des unbeabsichtigten Verlustes, der unbeabsichtigten Zerstörung und der unbeabsichtigten Schädigung beziehen sich wiederum auf Ereignisse, die vom Verantwortlichen nicht gewollt sind bzw. ohne Absicht stattfinden.[786] Der Verlust stellt dabei Fälle dar, in denen Daten(träger) verloren gehen oder gelöscht werden und eine Zerstörung liegt bspw. vor, wenn Datenträger vernichtet werden oder eine wesentliche Veränderung der Daten stattfindet.[787] Die unbeabsichtigte Schädigung ist ergänzend dazu als umfassende Auffangklausel zu sehen.[788]

12. Integrität und Vertraulichkeit bei der Verarbeitung von Wesensdaten

Um die Risiken einzudämmen, verlangt Art. 5 Abs. 1 lit. f DSGVO geeignete technische und organisatorische Maßnahmen. Diese werden gesetzlich in Art. 32 DSGVO konkretisiert. Im Zuge der Verarbeitung von Wesensdaten sind hier etliche Maßnahmen denkbar. Diese wurden detailliert bereits in Kapitel I.IV betrachtet.

13. Art. 5 Abs. 2 DSGVO: Rechenschaftspflicht

Art. 5 Abs. 2 DSGVO verpflichtet den Verantwortlichen dazu, die Grundsätze aus Abs. 1 einzuhalten. Diese Pflicht gliedert sich in zwei Bestandteile. Erstens muss der Verantwortliche dafür sorgen, dass die Grundsätze der

783 *Frenzel* (2021) BDSG, Art. 5 Rn. 46.
784 *Spindler/Dalby* (2019), Art. 5 DSGVO Rn. 15.
785 *Herbst* (2020), Art. 5 Rn. 74.
786 *Reimer* (2018), Art. 5 Rn. 51.
787 *Herbst* (2020), Art. 5 Rn. 75; *Reimer* (2018), Art. 5 Rn. 51.
788 *Reimer* (2018), Art. 5 Rn. 51.

Datenverarbeitung initial umgesetzt sowie fortführend eingehalten werden, und zweitens muss die Umsetzung ergänzend dokumentiert werden, damit diese auch nachgewiesen werden kann.[789] Art. 5 Abs. 2 DSGVO zwingt den Verantwortlichen demnach dazu, ein ganzheitliches Datenschutz-Managementsystem zu implementieren und dessen Status zu überwachen.[790]

Dieses Datenschutz-Managementsystem muss dabei so ausgestaltet sein, dass sich damit die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DSGVO nachweisen lassen. Dies ist besonders unter dem Gesichtspunkt des Art. 58 Abs. 1 lit. a DSGVO relevant, der Aufsichtsbehörden die Befugnis gibt, vom Verantwortlichen alle notwendigen Informationen zu erhalten.[791] Ergänzend dazu greift diese Nachweispflicht des Verantwortlichen auch in konkreten Streitfällen und führt hier zu einer Beweislastumkehr zu Gunsten von betroffenen Personen.[792] Da es für betroffenen Personen nur selten möglich ist, eindeutig zu beweisen, dass eine rechtswidrige Verarbeitung ihrer Daten vorliegt, ist es demnach die Pflicht des Verantwortlichen, darzulegen, dass seine Datenverarbeitung rechtmäßig ist.

Eine Konkretisierung der notwendigerweise zu ergreifenden Nachweismittel findet an vielen verschiedenen Stellen in der DSGVO statt. Besonders erwähnenswert sind dabei vor allem Art. 24 (technische und organisatorische Maßnahmen), Art. 28 Abs. 3 (Auftragsverarbeitungsverträge), Art. 30 (Verarbeitungsverzeichnis), Art. 33 f. (Meldung von Datenpannen) und Art. 35 DSGVO (Datenschutz-Folgenabschätzung).[793] Wie lange diese Nachweismittel vorgehalten und aufbewahrt werden müssen, wird allerdings nicht konkretisiert.[794] Eine dauerhafte Aufbewahrung ist demnach naheliegend, widerspricht allerdings dem risikobasierten Ansatz der DSGVO.[795] Auch formell macht die DSGVO keine Vorgaben dazu, wie die Nachweismittel vorgehalten werden müssen, wobei rein logisch eine schriftliche Dokumentation zu empfehlen ist.[796]

Sollte ein Verantwortlicher seiner Rechenschaftspflicht nicht nachkommen und die Einhaltung der Grundsätze nicht nachweisen können, könn-

789 *Roßnagel* (2019), Art. 5 Rn. 174.
790 *Frenzel* (2021) BDSG, Art. 5 Rn. 52.
791 *Herbst* (2020), Art. 5 Rn. 79.
792 *Pötters* (2018), Art. 5 Rn. 34.
793 Ein detaillierter Vorschlag zu den notwendigen Nachweismitteln: *Voigt* (2019), Art. 5 Rn. 41 ff.
794 *Herbst* (2020), Art. 5 Rn. 80; *Voigt* (2019), Art. 5 Rn. 44.
795 *Voigt* (2019), Art. 5 Rn. 44 - leitet darum einen dreijährige Aufbewahrungsfrist aus dem Ordnungswidrigkeitengesetz ab (OWiG).
796 *Herbst* (2020), Art. 5 Rn. 80; *Voigt* (2019), Art. 5 Rn. 45.

te dies gemäß Art. 83 Abs. 5 lit. a DSGVO mit einem Bußgeld von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs bestraft werden. Eine Haftungsbefreiung gemäß Art. 82 Abs. 3 DSGVO ist ohne Einhaltung der Rechenschaftspflicht ebenso ausgeschlossen.[797]

14. Rechenschaftspflicht bei der Verarbeitung von Wesensdaten

In dieser Arbeit wurde detailliert auf die technischen und organisatorischen Maßnahmen sowie auf die Datenschutz-Folgenabschätzung eingegangen. Dabei wurde gezeigt, welche Maßnahmen ergriffen werden können und wie eine Dokumentation zur Datenschutz-Folgenabschätzung aussehen sollte.

Auf Auftragsverarbeitungsverträge, Verarbeitungsverzeichnis und die Meldung von Datenpannen wurde nicht gesondert eingegangen. Grund dafür ist, dass diese Pflichten keine Besonderheit bei der Verarbeitung von Wesensdaten mittels BCI mit sich bringen und somit nicht relevant für die Beantwortung der Forschungsfrage sind. Demnach gilt auch für Verantwortliche, die Wesensdaten verarbeiten, dass diese entsprechende Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO dokumentieren, Datenpannen nach Art. 33 u. 34 DSGVO melden müssen sowie dafür verantwortlich sind, dass Auftragsverarbeitungsverträge i.S.v. Art. 28 Abs. 3 DSGVO abgeschlossen werden, sobald Dritte mit der Verarbeitung von Wesensdaten beauftragt werden.

797 *Herbst* (2020), Art. 5 Rn. 79.