I. Technischer und organisatorischer Datenschutz bei der Verarbeitung von Wesensdaten

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

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

I. Die Relevanz von Datensicherheit bei BCI

1. Die Lage der Cybersicherheit

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

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

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

496 *Ebenda.*

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

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

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

500 *Ebenda,* S. 61.

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

2. Cybersicherheit bei BCI

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

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

a. Vertraulichkeit

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

b. Integrität

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

---

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

c. Verfügbarkeit und Belastbarkeit

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

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

II. Art. 32 DSGVO: Technische und organisatorische Maßnahmen

1. Zweck und Inhalt der Reglung

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

2. Auswahlkriterien für geeignete Maßnahmen

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

a. Stand der Technik

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

b. Implementierungskosten

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

c. Art, Umfang, Umstand und Zweck der Verarbeitung

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

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

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

d. Eintrittswahrscheinlichkeit und Schwere des Risikos

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

3. Geeignete Maßnahmen

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

a. Pseudonymisierung und Verschlüsselung

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

b. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

c. Wiederherstellbarkeit

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

d. Kontrollverfahren

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

1. Zweck und Inhalt der Reglung

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

2. Beispiele für Datenschutz durch Technikgestaltung

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

1. Zweck und Inhalt der Reglung

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

---

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. Beispiele für datenschutzfreundliche Voreinstellungen

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

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

V. Adressat der Reglungen

1. Nur Verantwortliche verpflichtet

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

2. Probleme mit der alleinigen Verpflichtung von Verantwortlichen

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

VI. Technischer Datenschutz bei BCI

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

1. Bewertung von BCI

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

a. Art, Umfang, Umstände und Zwecke der Verarbeitung

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

b. Eintrittswahrscheinlichkeit und Schwere der Risiken

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

c. Stand der Technik und Implementierungskosten

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

a. Pseudonymisierung von Wesensdaten

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

b. Anonymisierung von Wesensdaten

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

c. Verschlüsselung

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

d. Angriffsschutz

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

e. Sichere Authentifizierung

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

f. Unterbindung von ständiger Aufzeichnung

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

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

---

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

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

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

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

g. Datenminimierung

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

h. Organisatorische Maßnahmen

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

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

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

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

3. Datenschutzfreundliche Voreinstellungen bei BCI

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

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

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

https://doi.org/10.5771/9783748971832-121 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY