J. Datenschutz-Management

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

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

I. Notwendigkeit einer Datenschutz-Folgenabschätzung

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

1. Hohes Risiko

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

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

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

a. Neue Technologien

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

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

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

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

b. Vorschlag der Art. 29-Gruppe

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

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

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

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

c. Zwingende Notwendigkeit einer DSFA

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

d. Vorgaben der Aufsichtsbehörden

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

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

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

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

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

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

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

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

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

II. Inhalt und Durchführung einer DSFA

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

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

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

---

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

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

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

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

1. Beschreibung der geplanten Verarbeitung

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

2. Bewertung der Notwendigkeit und Verhältnismäßigkeit

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

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

3. Risikobewertung

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

4. Abhilfemaßnahmen

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

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

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

5. Ergebnis der DSFA

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

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

6. Datenschutz-Folgeabschätzung bei BCI

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

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

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

a. Beschreibung der geplanten Verarbeitung

Verarbeitungszweck

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

Rechtsgrundlage

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

Kategorie betroffener personenbezogener Daten

Bei der Verarbeitung sind folgende personenbezogene Daten betroffen:

- Name
- Kontaktdaten
- Adressdaten
- Zahlungsdaten
- Wesensdaten

Kategorie betroffener Personen

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

Werden Auftragsverarbeiter eingesetzt? (inkl. Nennung)

Im konkreten Fall müssten hier alle Auftragsverarbeiter aufgelistet werden.

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

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

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

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

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

Im konkreten Fall müsste hier Entsprechendes aufgelistet werden.

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

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

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

Lebenszyklus der Daten

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

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

Welche Betriebsmittel werden eingesetzt?

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

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

b. Bewertung der Notwendigkeit und Verhältnismäßigkeit

Warum ist die Verarbeitung zwingend erforderlich?

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

Sind die Daten für die Verarbeitung zwingend erforderlich?

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

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

Warum ist die Verarbeitung verhältnismäßig?

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

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

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

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

Welche Speicherdauer haben die Daten?

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

c. Risikobewertung[709]

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

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

Tabelle 1: Risikomatrix

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

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

Tabelle 2: Übersicht der Risikoklassen

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

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

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

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

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

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

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

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

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

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

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

d. Ergebnis einer DSFA bei der Verarbeitung von Wesensdaten

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