

Sehr geehrte Vertreter*innen der psychotherapeutischen Berufsverbände,
sehr geehrte Mitverfasser*innen des Positionspapiers,
sehr geehrte Mitglieder des Psychotherapiebeirats,
sehr geehrte Kolleg*innen,

Stellungnahme und Kritik zum Positionspapier „Digitalisierung in der Psychotherapie in Österreich“

Executive Summary

Diese Stellungnahme versteht sich als ergänzender Diskussionsbeitrag zum Positionspapier „Digitalisierung in der Psychotherapie in Österreich“.

Ausgehend von eigener intensiver Auseinandersetzung mit KI-Systemen und digitalen Dokumentationslösungen werden drei zentrale Punkte kritisch beleuchtet:

- 1. Reale Datensicherheit und strukturelle Abhängigkeit von Anbietern:**
Insbesondere bei cloudbasierten SaaS-Lösungen stellt sich die Frage, ob sensible therapeutische Verlaufsdokumentationen tatsächlich technisch abgesichert sind oder letztlich auf Vertrauen in Anbieterstrukturen beruhen. Vor dem Hintergrund der gesetzlichen Verschwiegenheitspflicht erscheint hier eine vertiefte Auseinandersetzung notwendig.
- 2. Auswirkungen auf Ausbildung und professionelle Identitätsentwicklung:**
Der Einsatz KI-gestützter Analyse- und Dokumentationssysteme könnte langfristig verändern, wie therapeutische Kompetenz entsteht. Dokumentation, Selbstreflexion und der geschützte Lernraum in der Ausbildung sind zentrale Elemente professioneller Sozialisation und sollten nicht unbeabsichtigt verkürzt werden.
- 3. Ökonomisierung und Verschwiegenheit als Markenkern (USP):** Darüber hinaus wird der Zusammenhang zwischen Digitalisierung und möglichen Tendenzen zur Ökonomisierung psychotherapeutischer Praxis reflektiert. Die Psychotherapie sollte ihre Schutzstandards nicht unter Wettbewerbsdruck relativieren, sondern muss die absolute Verschwiegenheit als ihren professionsethischen Kern verteidigen.

Die Stellungnahme plädiert nicht für Technikverweigerung, sondern für eine sorgfältige, professionsethisch fundierte und strukturell abgesicherte Integration digitaler Systeme. Die hier formulierte Kritik richtet sich primär gegen cloudbasierte Systeme mit externer Verarbeitung hochsensibler Verlaufsdokumentationen – nicht gegen digitale Werkzeuge im Allgemeinen.

1. Einordnung und Ausgangspunkt

Das vorliegende Positionspapier stellt einen wichtigen und grundsätzlich begrüßenswerten Beitrag zur Auseinandersetzung mit Digitalisierung und Künstlicher Intelligenz (KI) im psychotherapeutischen Kontext dar. Es bietet eine differenzierte Darstellung von Chancen, Anwendungsfeldern und potenziellen Unterstützungsfunktionen.

Gerade weil ich mich in den vergangenen Monaten intensiv mit LLMs (u.a. ChatGPT, Gemini, Claude, ...), lokalen LLM-Architekturen, agentenbasierten Workflows und KI-gestützten Dokumentationssystemen auseinandergesetzt habe, sehe ich jedoch drei Kernbereiche, die im Positionspapier aus meiner Sicht nicht ausreichend kritisch beleuchtet werden:

1. **Reale Datensicherheit und Kontrollverlust gegenüber Anbietern**
2. **Auswirkungen auf Identitätsentwicklung und Kompetenzaufbau in der Ausbildung**
3. **Gefahr der Ökonomisierung und der Verlust der Verschwiegenheit**

Diese drei Aspekte betreffen nicht nur technische Detailfragen, sondern grundlegende Fragen unserer beruflichen Identität, unseres ethischen Auftrags und professionellen Verantwortung.

2. Datensicherheit: Die Illusion der technischen Beherrschbarkeit

2.1 Die „Black Box“ kommerzieller Anbieter

Das Positionspapier fordert „Privacy by Design“ sowie Ende-zu-Ende-Verschlüsselung. Diese Prinzipien sind normativ richtig - ihre tatsächliche technische Umsetzung bei kommerziellen Anbietern bleibt jedoch weitgehend intransparent.

Bei Systemen wie ChatGPT, Gemini oder vergleichbaren Plattformen haben wir als Psychotherapeut*innen **keine reale Kontrollmöglichkeit** darüber,

- wie Daten serverseitig verarbeitet werden,
- ob und in welcher Form sie für Trainingszwecke verwendet werden,
- welche Subunternehmer oder Cloud-Infrastrukturen involviert sind,
- wie lange Daten persistiert bleiben,
- welche Metadaten zusätzlich erhoben werden.

Selbst wenn Inhalte anonymisiert erscheinen, verbleiben sie in proprietären Systemarchitekturen, deren Funktionsweise wir nicht auditieren können. Damit entsteht

diplomatisch ausgedrückt ein Spannungsverhältnis zur gesetzlichen Verschwiegenheitspflicht, die nicht nur eine moralische, sondern auch eine rechtliche Ebene berührt.

Das Papier fordert Transparenz - bleibt jedoch vage, wo Transparenz technisch nicht herstellbar ist. Hier bedarf es klarer professionsethischer Grenzziehungen: Nicht jedes technologisch Mögliche ist im psychotherapeutischen Setting vertretbar.

Dabei ist zu beachten, dass der Begriff „Ende-zu-Ende-Verschlüsselung“ im Positionspapier undifferenziert verwendet wird. Ende-zu-Ende-Verschlüsselung bei einer laufenden Videokonferenz ist technisch etwas grundlegend anderes als die Verschlüsselung gespeicherter Verlaufsdaten in einer Cloud-Datenbank. Bei einer Videokonferenz werden Datenströme in Echtzeit zwischen zwei Endpunkten verschlüsselt – bei gespeicherten Daten hingegen stellt sich die Frage, wer den Schlüssel kontrolliert, wie Daten im Ruhezustand (at rest) geschützt sind und ob der Anbieter serverseitig Zugriff hat. Gerade diese Differenzierung wäre im Kontext therapeutischer Dokumentation essenziell, da sie Praktiker*innen vor einer falschen Sicherheit bewahren könnte. Wer liest „Ende-zu-Ende-Verschlüsselung“ und denkt: „Gut, dann ist es sicher“, dem fehlt möglicherweise das Bewusstsein dafür, dass der Anbieter bei den meisten Implementierungen dennoch Zugriff auf die Daten im Ruhezustand haben kann.

2.2 De-Anonymisierung durch biographische Dichte

Psychotherapeutische Dokumentation enthält eine hohe Verdichtung biographischer Informationen:

- seltene Lebensereignisse
- spezifische Kombinationen aus Beruf, Herkunft, Erkrankung, Beziehungsgeschichte
- zeitliche Abläufe

Selbst ohne explizite Namensnennung besteht ein erhebliches Re-Identifikationsrisiko durch Musterabgleich.

Algorithmen sind genau dafür optimiert: Mustererkennung über große Datensätze. Die Annahme, dass das Entfernen von Namen ausreichenden Schutz bietet, ist aus datenwissenschaftlicher Perspektive nicht haltbar.

Das Positionspapier erwähnt zwar mögliche Vertrauensverluste, verlagert die Schutzverantwortung jedoch weitgehend auf einzelne Therapeut*innen. De facto wird damit die systemische Risikostruktur individualisiert. Hier erwarte ich mir von einem

Berufsverband in einer Vertretungsrolle und Sprachrohr eine klarere Positionierung gegenüber „der (Konzern-) Technologie“.

2.3 „Human in the Loop“ – eine Scheinverantwortung?

Das Papier betont das Prinzip „Human in the Loop“. Die Letztverantwortung verbleibe beim Menschen.

Doch Verantwortung setzt Kenntnis und Kontrollfähigkeit voraus.

Wenn:

- Trainingsdaten unbekannt sind
- Entscheidungsarchitekturen (Model Weights, Prompt-Interpretation, Hidden Layer Dynamics) nicht prüfbar sind
- Modell-Updates ohne Einflussmöglichkeit erfolgen

dann übernehmen wir Verantwortung für ein System, dessen epistemische Grundlage wir nicht kennen.

Dies bedeutet nicht, dass Verantwortung unmöglich wäre – wohl aber, dass ihre Grundlage präzise geklärt werden sollte.

2.4 Lokale Modelle – begrenztes, aber realistisches Einsatzfeld

Eigene Experimente mit lokal betriebenen Sprachmodellen zeigen, dass KI-gestützte Strukturierung von Dokumentation technisch gut möglich ist, ohne Daten an externe Server zu übermitteln. Dieses Feld könnte perspektivisch ein sichereres Anwendungsgebiet darstellen. Ob es fachlich inhaltlich sinnvoll ist, werde ich in Punkt 3 kritisch betrachten.

An dieser Stelle möchte ich transparent machen, dass ich in diesem Papier zwei unterschiedliche Risikodimensionen aufzeigen versuche, die nicht verwechselt werden sollten: die datenschutztechnische Frage (wo werden Daten verarbeitet?) und die professionsethische Frage (was macht die Auslagerung von Reflexionsprozessen mit unserer Kompetenzentwicklung?). Lokale Modelle können die erste Dimension entschärfen, lassen die zweite jedoch unberührt. Wenn ich in Kapitel 3 die Auswirkungen auf den Reflexionsraum kritisch betrachte, gilt diese Kritik unabhängig davon, ob das Modell lokal oder extern läuft. Ich halte es für redlich, dieses Spannungsfeld offenzulegen, statt es argumentativ aufzulösen.

Aber auch hier gilt:

- Sicherheitsarchitektur
- Wartung

- IT-Kompetenz
- Haftungsfragen

müssten klar geregelt sein.

Derzeit fehlen – wie im Papier selbst richtigerweise gefordert – unabhängige Zertifizierungsstellen, klar definierte technische Standards und verbindliche Leitlinien. In dieser Situation wirkt eine implizite Ermutigung zur Nutzung entsprechender Systeme verfrüht.

Ein Kollege, der am Positionspapier mitgewirkt hat, hat in einem Online-Vortrag auf „theradocx“ verwiesen und auf mein Nachfragen hinsichtlich der Datensicherheit auf Verträge zwischen Psychotherapeut*in und Anbieter sowie auf die Einhaltung rechtlicher Vorgaben verwiesen.

Hier sehe ich jedoch eine strukturelle Problematik, die über vertragliche Zusicherungen hinausgeht.

Viele marktübliche SaaS-Anwendungen im Gesundheitsbereich sind so konzipiert, dass Passwort-Wiederherstellung, Support-Zugriff oder administrative Eingriffe technisch möglich bleiben müssen. Dies ist aus Nutzerfreundlichkeits- und Betriebsgründen nachvollziehbar. Gleichzeitig bedeutet es jedoch in der Regel, dass die Schlüsselverwaltung nicht ausschließlich in der Kontrolle der einzelnen Therapeutin bzw. des einzelnen Therapeuten liegt.

Solange ein System beispielsweise „Passwort-Reset ohne Datenverlust“ ermöglicht, ist zumindest davon auszugehen, dass serverseitige Mechanismen existieren, die prinzipiell einen Zugriffspfad eröffnen. Ob und wie dieser genutzt wird, ist eine Frage der Organisationspraxis – technisch ausgeschlossen ist er damit jedoch nicht zwingend.

Echte sogenannte „Zero-Knowledge“-Architekturen, bei denen selbst der Anbieter keinen Zugriff auf Inhalte hat, sind theoretisch möglich, in klassischen SaaS-Anwendungen jedoch selten anzutreffen, da sie mit erheblichen Einschränkungen (etwa unwiederbringlichem Datenverlust bei Passwortverlust) verbunden wären.

Mir geht es hier nicht um eine pauschale Unterstellung missbräuchlicher Zugriffe, sondern um eine nüchterne Feststellung: Solange die höchst sensible therapeutische Verlaufsdokumentationen(!) in extern betriebenen Cloud-Strukturen gespeichert werden, beruht ihre Vertraulichkeit nicht ausschließlich auf technischer Unzugänglichkeit, sondern wesentlich auf Vertrauen in Anbieterstrukturen.

Gerade im Kontext unserer gesetzlichen Verschwiegenheitspflicht stellt sich daher die Frage, ob ein vertrauensbasiertes Modell ausreicht – oder ob wir bei hochsensiblen Inhalten strengere Maßstäbe an technische Nicht-Zugreifbarkeit anlegen sollten.

So sehr ich innovative Projekte schätze und deren Engagement anerkenne: Bei der Speicherung hochsensibler Verlaufsdocumentationen oder gar der Verarbeitung laufender Therapiesitzungen durch externe KI-Systeme halte ich größte Zurückhaltung für geboten. Hier bewegen wir uns in einem Bereich, in dem die Risiken strukturell nicht allein durch Verträge oder Absichtserklärungen aufgehoben werden können.

2.5 Das Szenario des „Datenschatzes“: Kontrollverlust bei Unternehmensinsolvenz

Ein gravierender Mangel in der aktuellen Debatte ist das Fehlen eines „Exit-Szenarios“ für digitale Daten bei wirtschaftlichen Veränderungen der Anbieter. Cloudbasierte SaaS-Lösungen speichern hochsensible biographische Verläufe auf externen Servern. Im Falle einer Insolvenz oder eines Verkaufs des Anbieters stellen diese akkumulierten Daten einen erheblichen wirtschaftlichen Wert – einen regelrechten „Datenschatz“ – dar.

Im Falle von Insolvenz oder Eigentümerwechsel stellt sich die Frage, wie Datenhoheit und Löschkonzepte praktisch gesichert werden können. Es gibt derzeit keine technischen Garantien, dass diese Daten nicht als Teil der Konkursmasse an Dritte (z. B. Datenbroker, Tech-Giganten oder Versicherungen) veräußert werden, deren Interessen den psychotherapeutischen Grundwerten radikal widersprechen. Sobald ein Unternehmen schließt, verlieren Therapeut*innen jeglichen physischen und administrativen Zugriffspfad. Die im Positionspapier betonte „Datenhoheit“ der Patient*innen – und auch der Therapeut*innen – wird dadurch faktisch relativiert.

Ob und wie datenschutzrechtliche Verpflichtungen bei Insolvenz effektiv durchgesetzt werden können, bleibt praktisch schwer überprüfbar.

2.6 Das Aggregationsrisiko: Zentralisierung als qualitative Risikoverschiebung

Ein Aspekt, der im Positionspapier kaum adressiert wird, betrifft die qualitative Veränderung des Risikoprofils durch die Zentralisierung von Daten. In der analogen Welt lagern therapeutische Akten dezentral in hunderten Einzelpraxen. Ein Sicherheitsvorfall betrifft hier in der Regel die Akten einer einzelnen Praxis – typischerweise also einige Dutzend bis wenige hundert Patient*innen.

Bedient ein cloudbasierter SaaS-Anbieter jedoch beispielsweise 1.000 Therapeut*innen, die jeweils 30 Patient*innen dokumentieren, liegen 30.000 vollständige biographische Verläufe an einem einzigen, zentralen Ort. Dies stellt nicht nur eine quantitative, sondern eine fundamentale qualitative Veränderung dar: Es entsteht ein aggregierter Datensatz von immensem Wert – hochinteressant für Versicherungen, Arbeitgeber oder datengetriebene Geschäftsmodelle. Dass einige Anbieter bereits offensiv mit hohen Nutzungszahlen im therapeutischen Bereich werben, unterstreicht die rasante Realität dieser Aggregation.

Das unter Punkt 2.5 beschriebene „Insolvenz-Szenario“ gewinnt durch diese Bündelung eine zusätzliche, bedrohliche Brisanz: Im Ernstfall verliert nicht mehr eine einzelne Praxis, sondern ein relevanter Teil unseres gesamten Berufsstandes die Kontrolle über seine sensibelsten Daten. Diese strukturelle Verschiebung des Risikoprofils – von einer verteilten, begrenzten hin zu einer zentralisierten, systemischen Verwundbarkeit – wird in der aktuellen Debatte noch völlig unterschätzt. Es handelt sich um ein emergentes Risiko, das durch die bloße Summierung individueller Nutzungsentscheidungen entsteht, ohne dass wir als Profession noch eine übergeordnete Steuerungsmöglichkeit hätten.

Die medialen und gesellschaftlichen Auswirkungen, die ein massives Datenleck oder ein gravierender Sicherheitsvorfall bei einem großen kommerziellen SaaS-Anbieter für das Vertrauen in die Psychotherapie hätte, wären schlichtweg verheerend.

3. Ausbildung und Identitätsentwicklung: Eine unterschätzte Gefahr

Weiters erscheinen mir die Auswirkungen auf die Entwicklung angehender Psychotherapeut*innen als potentielle Gefahr.

3.1 Verlust therapeutischer Intuition

Das Papier hebt hervor, dass KI Allianz-Rupturen oder Interaktionsmuster erkennen könne.

Gerade in der Ausbildung ist es jedoch zentral, Spannungen:

- wahrzunehmen
- auszuhalten
- im eigenen Körper zu spüren
- im intersubjektiven Feld zu reflektieren

Wenn Rückmeldungen externalisiert werden - etwa durch automatisierte Musteranalysen – verschiebt sich der Lernort vom Beziehungsgeschehen zum Bildschirm.

Es könnte zu einer Verschiebung der therapeutischen Kernkompetenz zu algorithmischer Signalgebung kommen. Daher ist der Einsatz mit viel Bedacht zu wählen. Er kann ergänzen, sollte aber niemals ersetzen. Selbst testete ich KI auch zur „eigenen Supervision therapeutischen Arbeitens“ und die Ergebnisse waren durchaus erweiternd und faszinierend. Aufgrund der im Punkt 2.2. benannten „De-Anonymisierung“ habe ich aber mittlerweile jedoch davon mehr Abstand genommen.

3.2 KI-„Hörigkeit“ statt professioneller Selbstwirksamkeit

Ausbildung ist eine Phase erhöhter Unsicherheit. Wenn ein „intelligentes System“ scheinbar objektives Feedback liefert, entsteht leicht eine epistemische Verschiebung:

- vom eigenen Wahrnehmen
- zur technischen Autorität

Das Papier spricht von „evidenzbasierter Qualität“, unterschätzt jedoch, dass Psychotherapie kein datenanalytisches Optimierungsproblem ist, sondern ein intersubjektiver Prozess.

Therapie erschöpft sich nicht in Mustererkennung.

3.3 Dokumentation als Lernprozess

Dokumentation ist in der Ausbildung kein rein administrativer Akt. Sie ist ein zentraler Reflexionsraum. Im Schreiben verdichtet sich Wahrnehmung, entstehen Hypothesen, wird Theorie mit Praxis verbunden. Dieser Prozess trägt wesentlich zur Entwicklung einer professionellen Identität bei. Dokumentieren ist:

- Verdichtung von Wahrnehmung
- Selbstreflexion
- Theoriebildung
- Strukturierung des eigenen Denkens

Wird dieser Prozess ausgelagert, wird nicht nur Zeit gespart - es geht ein zentraler Reflexionsraum verloren.

Gerade in Ausbildung unter Supervision ist dieser Raum konstitutiv für Rollenfindung.

3.4 Überwachungskultur statt geschütztem Lernraum

Ähnliches gilt für KI-gestützte Videoanalysen oder automatisierte Auswertungen. Auch wenn sie zusätzliche Perspektiven liefern können, entsteht potenziell eine Kultur permanenter Bewertung. Professionelles Wachstum benötigt jedoch geschützte Räume, in denen Unsicherheit, Irrtum und Suchbewegungen möglich sind, ohne unmittelbar in Leistungskennzahlen übersetzt zu werden. Psychotherapieausbildung darf nicht zu einem datengestützten Leistungsmonitoring werden. Daher sollte gerade im Ausbildungskontext besonders sorgfältig abgewogen werden, welche Formen technischer Unterstützung sinnvoll sind und welche möglicherweise unbeabsichtigte Nebenwirkungen haben.

3.5 Die „Schein-Einwilligung“: Machtgefälle und therapeutische Compliance Das Positionspapier setzt stark auf das Prinzip der „informierten Entscheidung“ und die Autonomie der Patient*innen. Dabei wird jedoch die spezifische psychodynamische Situation im psychotherapeutischen Setting vernachlässigt: Patient*innen befinden sich oft in einer gewissen Form der Abhängigkeitsbeziehung zur Therapeutin oder zum Therapeuten. Die Bitte, einer KI-gestützten Dokumentation oder Analyse zuzustimmen, kann einen massiven Druck erzeugen. Ein „Ja“ erfolgt hier häufig nicht aus technischer Überzeugung, sondern um die therapeutische Allianz nicht zu gefährden oder die Bezugsperson nicht zu enttäuschen (Compliance).

Besonders Menschen in akuten Krisen oder vulnerablen Zuständen verfügen oft nicht über die notwendigen Ressourcen, um die lebenslangen Konsequenzen einer digitalen Datenpersistenz rational abzuwägen. Hier greift unsere unbedingte Fürsorgepflicht, die nicht durch eine bloße Unterschrift (Informed Consent) auf die Patient*innen delegiert werden darf. Zudem verändert das bloße Wissen um einen „digitalen Dritten“ (die KI), der permanent mitliest oder -hört, den intersubjektiven Raum. Die notwendige „Hemmungslosigkeit“ des Mitteilens droht einer bewussten oder unbewussten Selbstzensur zu weichen. In meinem psychodramatischen Verständnis stellt sich die Frage, wie sich KI als Intermediär- oder Intramediärobject so integrieren ließe, dass sie am Ende der Aktionsphase wieder ihren ursprünglichen, bedeutungsarmen Zustand erreicht. Wenn die KI jedoch Daten speichert, behält sie „Bedeutung“.

3.6 Strukturelle Verantwortung vs. individuelle Kompetenzanforderungen an Lehrtherapeut*innen Das Positionspapier definiert einen umfangreichen Anforderungskatalog an „Kernkompetenzen“, die Lehrtherapeut*innen für die Supervision und Lehre im digitalen Setting künftig erfüllen sollen. Dieser umfasst unter anderem die eigenständige Evaluierung von Ende-zu-Ende-Verschlüsselungen und Zugriffsmanagement bei Videodiensten, die Vorhaltung technischer Notfall-Fallbacks sowie die profunde Beurteilung von Bias- und Datenschutzrisiken bei KI-Modellen.

Bei sachlicher Betrachtung stellt dieser Katalog eine erhebliche Rollenverschiebung dar. Die fundierte Expertise von Lehrtherapeut*innen liegt in ihrer langjährigen psychotherapeutischen Praxis, der Beziehungsgestaltung und der didaktischen Weitergabe psychotherapeutischer Kompetenzen. Die implizite Forderung, Lehrende müssten künftig in der Lage sein, komplexe algorithmische Systeme auf ihre Datensicherheit hin zu auditieren, verlagert ein systemisches Problem auf die individuelle Ebene.

Anstatt die Verantwortung für die Prüfung und Absicherung technischer Infrastrukturen zu individualisieren, bedarf es hier zentraler, struktureller Lösungen. Notwendig sind verbandsseitig oder staatlich zertifizierte, sofort sicher einsetzbare Systeme („Plug &

Play“). Nur durch eine solche strukturelle Entlastung kann sichergestellt werden, dass sich erfahrene Ausbilder*innen – ungeachtet ihrer individuellen IT-Affinität – weiterhin auf ihre pädagogischen und therapeutischen Kernaufgaben konzentrieren können. Andernfalls besteht das Risiko, dass der wertvolle Erfahrungsschatz insbesondere älterer Kolleg*innen für die Ausbildung verloren geht, weil Hürden aufgebaut werden, die primär in den Bereich der IT-Administration fallen.

4. Gefahr der Ökonomisierung therapeutischer Praxis

Implizit entsteht der Eindruck, dass Effizienzsteigerung und Prozessoptimierung leitende Motive sind:

- schnellere Dokumentation
- strukturierte Verlaufsanalysen
- quantitative Auswertbarkeit

Diese Argumente sind nachvollziehbar. Gleichzeitig entsteht die Frage, welche Haltung hier mitschwingt. Aus meiner Sicht ist Psychotherapie kein skalierbares Marktprodukt, sondern ein Begegnungsraum.

Wenn technische Systeme zunehmend Prozesse strukturieren, besteht die Gefahr, dass wir – bewusst oder unbewusst – zu „therapeutischen Funktionsinstanzen“ in einem digital verwertbaren System werden.

Der ÖAGG hat für März 2026 zu einer außerordentlichen Generalversammlung eingeladen und dabei unter anderem diese zentralen Fragen formuliert:

- Wie begegnen wir der Entwicklung von Psychotherapie und psychosozialer Beratung als Geschäftsmodell?
- Welche Verantwortung tragen wir gegenüber vulnerablen Gruppen?

Diese Fragen stehen in engem Zusammenhang mit der Digitalisierung. Wenn psychotherapeutische Prozesse zunehmend standardisiert, messbar und auswertbar werden, verändert sich potenziell auch ihr gesellschaftlicher Rahmen.

Häufig wird argumentiert, die Psychotherapie müsse sich dem technologischen Tempo anpassen, um nicht von unregulierten Coaching-Apps oder KI-Chatbots verdrängt zu werden. Diesem Narrativ muss widersprochen werden: Die gesetzliche Verschwiegenheitspflicht ist kein technisches Hindernis, das es zu überwinden gilt, sondern unser höchstes Gut und unser absolutes Alleinstellungsmerkmal (USP, Marketingsprache). Wenn die Psychotherapie ihre Schutzstandards senkt, um mit „niederschwelligen“ digitalen Angeboten des freien Marktes zu konkurrieren, verliert sie ihre ethische Integrität und ihren „Markenkern“. Ein bewusster Verzicht auf strukturell

unsichere KI-Systeme ist kein Rückschritt, sondern eine Form der Qualitätssicherung in einer zunehmend gläsernen Gesellschaft. Besonders gegenüber vulnerablen Gruppen tragen wir eine hohe Verantwortung. Sie dürfen nicht zu Datenlieferant*innen in einem System werden, dessen Logik primär ökonomisch oder technologisch geprägt ist.

Gleichzeitig ist mir bewusst, dass diese Position ein Spannungsfeld eröffnet, das nicht verschwiegen werden darf: Das Positionspapier weist völlig zu Recht darauf hin, dass digitale Formate existierende Versorgungslücken schließen können – etwa in ländlichen Regionen, für mobilitätseingeschränkte Personen oder bei stark schambesetzten Themen. Dieser Versorgungsbedarf ist unbestreitbar und jede strukturelle Zurückhaltung bei der Digitalisierung hat ihren Preis, der sich in Form von Wartezeiten, mangelnder Erreichbarkeit und unadressiertem Leidensdruck konkretisiert.

Meine Forderung nach einem vorsichtigeren Vorgehen darf nicht als Gleichgültigkeit gegenüber diesem Leidensdruck gelesen werden. Im Gegenteil: Gerade weil Menschen in vulnerablen Situationen auf verlässliche Hilfe angewiesen sind, dürfen wir ihnen keine Systeme anbieten, deren Sicherheit wir nicht garantieren können. Die Dringlichkeit der Versorgung rechtfertigt keine Kompromisse bei der Vertraulichkeit – sie erhöht vielmehr den Druck, sichere Lösungen schneller zu schaffen, anstatt kommerzielle Marktlösungen vorschnell zu normalisieren.

5. Haltung: Technikoffen, aber professionsschützend

Ich verstehe mich selbst als technikaffin und innovationsfreundlich. Ich nutze KI privat intensiv und sehe ihr Potenzial klar.

Gerade deshalb sehe ich aber auch mögliche Kehrseiten:

- die immense Geschwindigkeit der Entwicklung
- die wirtschaftlichen Interessen dahinter
- die strukturelle Intransparenz (großer) Anbieter
- die Tendenz zur schleichenden Normalisierung

Die Psychotherapie braucht hier einen konservativen Schutzraum - nicht im Sinne von Technikverweigerung, sondern im Sinne eines ethischen Innehaltens.

Was sich gesellschaftlich durchsetzt, muss nicht automatisch professionsethisch integrierbar sein.

Ich habe mir mehrere SaaS-Lösungen für Praxisverwaltung, die mittels einer einfachen Google-Suche, schnell recherchierbar sind, angesehen und teils auch mit Testaccounts getestet. Sowohl die beworbenen Versprechen und Marketingmaßnahmen als auch die Rezensionen von Nutzer*innen und technische Umsetzungen zeigen aus meiner Sicht

einen deutlichen professionspolitischen Klärungsbedarf. Einige Anbieter werben mit hohen Nutzungszahlen im therapeutischen Bereich. Dies verdeutlicht, dass faktisch bereits eine breite Implementierung stattfindet – ohne dass unabhängige Zertifizierungsmechanismen etabliert sind.

Abschließend zu meiner Haltung: Ich bin mir bewusst, dass ich in dieser Stellungnahme Probleme benenne, ohne für jedes Einzelne eine fertige Lösung anzubieten. Dies ist kein Versäumnis, sondern Ausdruck meines Verständnisses eines solchen Diskussionsbeitrags. Die Entwicklung von Zertifizierungsstandards, sicheren technischen Architekturen und verbindlichen professionsethischen Leitlinien ist ein kollektiver Prozess, der weder von einer Einzelperson geleistet werden kann noch soll. Ich sehe meine Rolle an dieser Stelle darin, blinde Flecke aufzuzeigen und kritische Fragen zu formulieren. An der konstruktiven Erarbeitung von Lösungen beteilige ich mich jederzeit gerne – doch ich erwarte von einem Berufsverband und staatlichen Gremien, dass er diesen Prozess strukturiert, moderiert und professionell ermöglicht. Dazu gehört auch, wichtige Zwischenergebnisse klar nach außen an uns Psychotherapeut*innen, Klient*innen sowie an gesundheitspolitisch und gesellschaftlich relevante Institutionen zu kommunizieren.

6. Forderungen

Solange folgende Voraussetzungen nicht erfüllt sind:

- unabhängige Zertifizierungsstellen für cloudbasierte Verarbeitung
- technisch nachvollziehbare Sicherheitsstandards
- garantierte und überprüfbare Löschkonzepte, die auch bei Unternehmensinsolvenz oder Marktaustritt des Anbieters greifen, sowie die Rückgabe bzw. Herausgabe der Daten garantieren
- verbindliche Datenschutz-Audits
- differenzierte Fortbildungen mit technischer Tiefenschärfe
- klare Negativabgrenzungen ungeeigneter Systeme (und hier sind aktuelle einige am „Markt“)
- tiefe Berücksichtigung der psychodynamischen Auswirkungen (Übertragung/Compliance) vor der Einholung von Einwilligungen der Patient*innen und Klient*innen
- eine Risikobewertung, die das Aggregationsrisiko zentralisierter Datenhaltung berücksichtigt und Obergrenzen oder strukturelle Schutzmechanismen gegen übermäßige Datenkonzentration bei einzelnen Anbietern vorsieht

sollte:

- vom Einsatz externer cloudbasierter Systeme – insbesondere solcher mit integrierten KI-Funktionen – im Kontext therapeutischer Dokumentation und Prozessanalyse klar abgeraten werden
- in Ausbildungskontexten sehr zurückhaltend vorgegangen werden
- die Priorität auf professionsethischer Identitätsbildung liegen
- eine ehrliche, differenzierte Risikokommunikation an Kolleg*innen erfolgen, die nicht suggeriert „es ist sicher“, sondern transparent benennt, „unter folgenden Bedingungen ist es sicherer als bestimmte Alternativen, aber hier sind die durchaus massiven Risiken, die Sie kennen müssen“

Innovative Konzepte mögen technisch faszinierend sein. Ohne überprüfbare Sicherheit bleiben sie jedoch riskant.

7. Schlussbemerkung

Die Auseinandersetzung mit KI ist notwendig und sinnvoll. Was jedoch vermieden werden muss, ist eine vorschnelle Integration unter dem Eindruck technologischer Dynamik. Psychotherapie ist ein hochsensibler Raum, getragen von:

- Vertrauen
- Verschwiegenheit
- leiblich-emotionaler Resonanz
- intersubjektiver Erfahrung

Diese Grundlagen dürfen nicht durch eine Entwicklung überrollt werden, deren strukturelle Logik primär datenökonomisch ist.

Diese Stellungnahme versteht sich als Einladung zum Weiterdenken. Die Fragen, die ich stelle, sind nicht rhetorisch gemeint – sie verlangen nach Antworten, die nur gemeinsam erarbeitet werden können. Ich würde es begrüßen, wenn die hier aufgeworfenen Punkte – insbesondere das Aggregationsrisiko zentralisierter Datenhaltung, die psychodynamische Problematik der Einwilligungssituation und die ehrliche Auseinandersetzung mit dem Status quo analoger Datensicherheit – in die weitere Diskussion, in künftige Fassungen des Positionspapiers sowie in akut notwendige, klare Handlungsempfehlungen für unsere Kolleg*innen einfließen.

Mit freundlichen Grüßen

Alexander Ortner