

702

Geldwäscheprävention



**PHILIPP L. LEITNER**  
 Der Autor ist Rechtsanwalt bei SCWP Schindhelm in Linz und Lektor an der Johannes Kepler Universität Linz sowie an der IMC Fachhochschule Krems.

2023/333

# Mit KI und Automation im anwaltlichen Betrieb gegen Geldwäsche und Terrorismusfinanzierung

## I. EINLEITUNG

Rechtsanwältinnen und Rechtsanwälte sind nach Maßgabe der §§ 8 a ff RAO<sup>1</sup> verpflichtet, ein wirksames Compliance-System einzurichten, um im Rahmen der Abwicklung eines Mandats Geldwäscherei (ML) und Terrorismusfinanzierung (FT) erkennen und verhindern zu können. Ein solches System erstreckt sich – neben allgemeinen Sorgfaltspflichten<sup>2</sup> – auf kanzleibezogene Sorgfaltspflichten<sup>3</sup> wie bspw die Durchführung einer allgemeinen Kanzlei-Risikoanalyse (§ 8 a Abs 3 RAO) oder die Einrichtung eines internen Whistleblowing-Systems (§ 9 Abs 8 RAO). Auf Mandantenebene umfasst es etwa die Prüfung, ob ein geldwäschegeneigtes Geschäft vorliegt (§ 8 a Abs 1 RAO), samt dessen eingehender Überprüfung im Anlassfall (§ 8 b Abs 6 RAO), die Durchführung des KYC-Prozesses (§ 8 b Abs 1 RAO) sowie die Erstattung einer allfälligen Verdachtsmeldung an die Geldwäschemeldestelle (§ 8 c Abs 1 RAO; via goAML).<sup>4</sup> Eine Verletzung dieser anwaltlichen Verpflichtungen ist sowohl berufsrechtlich<sup>5</sup> als auch strafrechtlich<sup>6</sup> sanktioniert. In ihrer grenzüberschreitenden Risikobewertung vom Oktober 2022 hob die Europäische Kommission hervor, dass das Risiko von ML bzw FT im rechtsberatenden Bereich als „signifikant“ (Level 3) angesehen wird.<sup>7</sup> Ein hoher Standard bei der Einführung und Aufrechterhaltung von Compliance-Maßnahmen ist daher geboten; Softwareapplikationen, die auf Automatisierungsmechanismen sowie fortgeschrittene Technologien wie bspw künstliche Intelligenz zurückgreifen, können dabei maßgeblich unterstützen.

Die Nutzung fortgeschrittener Technologien ist jedenfalls im Bankenbereich verbreitet. Bereits 2020 empfahl die EU-Bankenvereinigung den verstärkten Einsatz von künstlicher Intelligenz zur Unterstützung von Experten.<sup>8</sup> Auch die Financial Action Task Force on Money Laundering (FATF) identifizierte bereits im Jahr 2021 insbesondere künstliche Intelligenz sowie Natural Language Processing (NLP)<sup>9</sup> als zukunftsweisende Technologien zur Verhinderung von ML und FT.<sup>10</sup> Mit der Novellierung des FM-GwG<sup>11</sup> im Jahr 2021 wurde § 7 a FM-GwG eingefügt.<sup>12</sup> Gemäß dessen Abs 1 darf ein aufgrund des FM-GwG einzurichtendes Transaktionsmonitoring „unter Verwendung eines auf künstlicher Intelligenz oder anderen fortschrittlichen Technologien<sup>13</sup> basierenden Ansatzes durchgeführt oder ergänzt werden“.<sup>14</sup> Die FMA hob in ihrem Schwerpunktbericht 2022 hervor, dass das Ausmaß an Digitalisierung zur Verhinderung von ML und FT im Jahr 2023 zunehmen

wird, wobei Unternehmen insbesondere künstliche Intelligenz zum Transaktionsmonitoring sowie zur Risikoklassifizierung heranziehen; gleichsam steigt auch deren Bedeutung in der Aufsicht.<sup>15</sup>

Gegenstand dieses Beitrags ist die Darstellung des derzeitigen Rechtsrahmens für den Einsatz von Legal Tech zur Verhinderung von ML und FT. Im Sinne eines Pflichtenhefts werden abschließend Vorschläge zur Automatisierung von Prozessen bzw intelligenten Datenverarbeitung zur Diskussion gestellt.

## II. ZUM BEGRIFF DER „KÜNSTLICHEN INTELLIGENZ“

Wenngleich der Begriff „künstliche Intelligenz“ nicht neu ist,<sup>16</sup> konnte sich eine einheitliche, rechtsverbindliche Defi-

<sup>1</sup> Rechtsanwaltsordnung (RAO), RGBl 96/1868 idF BGBl I 2023/39.  
<sup>2</sup> Lehner/Vitek in Engelhart/Hoffmann/Lehner/Rohregger/Vitek (Hrsg), RAO<sup>11</sup> § 8 a Rz 9 (Stand 1. 11. 2022, rdb.at).  
<sup>3</sup> Lehner/Vitek in RAO (FN 2) § 8 a Rz 10.  
<sup>4</sup> Österreichischer Rechtsanwaltskammertag (Hrsg), Verhinderung von Geldwäsche und Terrorismusfinanzierung in Anwaltskanzleien: Information und Leitfaden für Rechtsanwälte (Stand Jänner 2022) 32.  
<sup>5</sup> Geldbuße bis zum Betrag von € 45.000,-, im Falle schwerwiegender, wiederholter oder systematischer Verstöße bis zu € 1.000.000,-, § 16 Abs 1 Z 2 DSt; ebenso Veröffentlichung der Verurteilung auf der Website der Rechtsanwaltskammer unter Identitätspreisgabe für die Dauer von zumindest fünf Jahren, § 70 Abs 3 DSt.  
<sup>6</sup> Insb Beihilfe zur Geldwäscherei nach § 165 StGB, vgl Österreichischer Rechtsanwaltskammertag, ÖRAK-Leitfaden (FN 4) 8.  
<sup>7</sup> Europäische Kommission, Annex 1 zum Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der mit grenzüberschreitenden Tätigkeiten im Zusammenhang stehenden Risiken der Geldwäsche und der Terrorismusfinanzierung für den Binnenmarkt, COM(2022) 554 final, 199.  
<sup>8</sup> Teichmann/Falkner, Die Empfehlungen der EBF zu effektiveren Anti-Geldwäsche -Maßnahmen, CB 2021, 416 (417f) mwN EBF, Lifting the Spell of Dirty Money: EBF blueprint for an effective EU framework to fight money laundering. <https://www.ebf.eu/wp-content/uploads/2020/03/EBF-Blueprint-for-an-effective-EU-framework-to-fight-money-laundering-Lifting-the-Spell-of-Dirty-Money-.pdf> (abgefragt 20. 10. 2023).  
<sup>9</sup> Computerlinguistik.  
<sup>10</sup> FATF, Opportunities and Challenges of New Technologies for AML/CFT (July 2021), Rz 80, 82, <https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html> (abgefragt 20. 10. 2023).  
<sup>11</sup> Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG), BGBl I 2016/118 idF BGBl I 2021/98.  
<sup>12</sup> BGBl I 2021/25.  
<sup>13</sup> Gemeint sind damit beispielsweise Netzwerkanalysen, Graphenalgorithmen oder Alert Scoring/Triagemodelle, s IA 1191/A, 27. GP 17.  
<sup>14</sup> Soweit die in § 7 a Abs 2 FM-GwG genannten Voraussetzungen eingehalten werden; vertiefend Gorzala, Neues EU-Geldwäschepaket und der Einsatz künstlicher Intelligenz zur Geldwäscheprävention, ÖBA 2021, 703 (706).  
<sup>15</sup> Österreichische Finanzmarktaufsicht, Themenschwerpunkte und Trends 2022: Prävention von Geldwäsche und Terrorismusfinanzierung 22, <https://www.fma.gv.at/querschnittsthemen/geldwaescherei-und-terrorismusfinanzierung/> (abgefragt 20. 10. 2023).  
<sup>16</sup> Der Begriff wurde als Beschreibung der wissenschaftlichen Disziplin für ein universitäres Sommerprojekt erstmals im Jahr 1955 definiert, vgl McCarthy/Minsky/Rochester/Shannon, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence (31. 08. 1955) 2, [jmc.stanford.edu/articles/dartmouth/dartmouth.pdf](https://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf) (abgefragt 20. 10. 2023).

nition jedoch insbesondere im Hinblick auf die Vielzahl unterschiedlicher technischer Verfahren, die unter diesem gemeinsamen begrifflichen Dach zusammengefasst werden, bislang noch nicht herausbilden.<sup>17</sup> Im Bereich von ML und FT findet „künstliche Intelligenz“ in § 7a Abs 1 FM-GwG iZm Transaktionsmonitoring ausdrücklich Erwähnung; eine nähere Erläuterung, was unter dem Begriff im Detail verstanden wird, lassen sowohl der Gesetzestext als auch die Erläuterungen offen.<sup>18</sup>

In ihrem Strategiepaper aus dem Jahr 2021 definierte die FATF künstliche Intelligenz als „Wissenschaft, menschliche Denkfähigkeiten nachzuahmen, um Aufgaben auszuführen, die typischerweise menschliche Intelligenz erfordern, zB Muster erkennen, Empfehlungen oder Entscheidungen abgeben“, wobei „fortschrittliche Computertechniken“ zur Anwendung kommen, um Erkenntnisse aus unterschiedlichen Datentypen zu erhalten, damit „autonom Probleme gelöst und Aufgaben ausgeführt werden. [...]“.<sup>19</sup> Nach diesem Definitionsansatz wären bloße Automatismen (iSv deterministischen Wenn-Dann-Funktionen) nicht von diesem Begriff umfasst.

Im April 2021 veröffentlichte die Europäische Kommission zudem einen ersten Entwurf einer KI-Verordnung,<sup>20</sup> mit welcher eine Klassifizierung von KI-Systemen – unter Anwendung eines differenzierten Normenregimes je nach Art des KI-Systems – vorgesehen ist. Problematisch ist dabei die Definition eines solchen KI-Systems. Im aktuellen, dem Trilog-Verfahren zur Diskussion zugrunde liegenden Entwurf<sup>21</sup>, wird ein solches – etwas sperrig – als „maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und das für explizite oder implizite Ziele Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das physische oder virtuelle Umfeld beeinflussen“, bezeichnet.<sup>22</sup> Dieser Definitionsansatz birgt die Gefahr einer ausufernden Klassifikation technischer Systeme als „KI-Systeme“.<sup>23</sup> Inwieweit im Trilog-Verfahren noch eine angemessene Eingrenzung erfolgt, wird sich zeigen.<sup>24</sup>

Wenngleich das Datenschutzrecht den Begriff der „künstlichen Intelligenz“ nicht kennt, nimmt es zumindest indirekt darauf Bezug.<sup>25</sup> Mit Art 22 DSGVO wird für „automatisierte Entscheidungen im Einzelfall einschließlich Profiling“ ein besonderer Rechtsrahmen vorgesehen; im Wesentlichen handelt es sich dabei um (maschinelle) Entscheidungen, die „ausschließlich auf einer automatisierten Verarbeitung“ beruhen, sodass eine menschliche Mitwirkung aus inhaltlicher Sicht völlig unterbleibt oder sich auf rein formale Aspekte („Abnicken“ ohne nähere Prüfung) reduziert.<sup>26</sup> Die Entscheidung muss zudem gegenüber der betroffenen Person eine „rechtliche Wirkung entfalte[n] oder sie in ähnlicher Weise erheblich beeinträchtigt [en]“ (Abs 1 leg cit). Im Bereich ML sowie FT ist dies dann der Fall, wenn bspw eine (rein maschinelle) Entscheidung getroffen würde, ein Mandat aufgrund Compliance-Beden-

ken nicht zu übernehmen oder eine Verdachtsmeldung an die Geldwäschemeldestelle zu erstatten.<sup>27</sup> Mit Blick auf das eingangs genannte Transaktionsmonitoring (§ 7a FM-GwG) ist anzumerken, dass dieses nach den Erläuterungen ausdrücklich nicht als automatisierte Entscheidungsfindung im Einzelfall gelten soll, zumal dessen Ergebnis (Liste mit auffälligen Transaktionen) als Vorschlag einer weiterführenden menschlichen Entscheidung bedürfen soll.<sup>28</sup>

### III. RECHTLICHE RAHMENBEDINGUNGEN

#### 1. Technischer Rahmen nach der Rechtsanwaltsordnung (RAO)

Konkrete Rahmenbedingungen, welcher Grad an Automatisierung im Rahmen des verpflichtend einzurichtenden Compliance-Systems erlaubt ist, bzw ob und ggf welche Schranken für den Einsatz fortgeschrittener Technologien wie künstliche Intelligenz bestehen, sind in den §§ 8a ff RAO nicht enthalten. Insbesondere fehlt eine dem § 7a FM-GwG nachgebildete Parallelbestimmung.

In den gesetzlichen Bestimmungen wird vielmehr extensiv auf dynamische und auslegungsbedürftige Rechtsbegriffe zurückgegriffen.<sup>29</sup> So wird beispielsweise dem Rechtsan-

<sup>17</sup> Vgl Niederée/Nejdl in Ebers/Heinze/Krügel/Steinrötter (Hrsg), Künstliche Intelligenz und Robotik (2020) § 2 Rz 1; Ertel, Grundkurs Künstliche Intelligenz<sup>4</sup> (2016) 1ff.

<sup>18</sup> Siehe auch IA 1191/A, 27. GP 17f; dies ist im Übrigen kein isoliertes Problem des FM-GwG, sondern zeigt sich auch in anderen Rechtsmaterien, wie bspw in § 2 Abs 2 Z 4 DSFA-V.

<sup>19</sup> FATF, Opportunities and Challenges (FN 10), Rz 78.

<sup>20</sup> Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM/2021/206 final (21. 4. 2021).

<sup>21</sup> Änderungen des Europäischen Parlaments zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, P9\_TA (2023)0236 (14. 06. 2023).

<sup>22</sup> Abänderung 165 des KI-Verordnungsentwurfs idF vom 14. 6. 2023 (FN 21).

<sup>23</sup> Demgemäß könnte möglicherweise bereits ein (schlichter) Automatismus, beispielsweise die Erkennung des Worts „Liegenschaftskaufvertrag“ in einem Suchbegriff eines elektronischen Akts oder in einem Word-Dokument, das in einem solchen Akt enthalten ist, unter anschließender automatischer Befüllung eines Formulars, als KI-System gelten.

<sup>24</sup> Dies auch vor dem Hintergrund, dass KI-Systeme, die zur Verhinderung von ML und FT eingesetzt werden, (wohl) Hochrisiko-KI-Systeme darstellen (Anhang III Z 6 lit g des KI-Verordnungsentwurfs idF vom 14. 6. 2023 [FN 21]) und demnach einem besonders strengen Rechtskorsett unterliegen; s dazu näher Kapitel 2 des KI-Verordnungsentwurfs idF vom 14. 6. 2023 (FN 21), insb die Verpflichtung zur Implementierung eines Risikomanagementsystems (Art 9 leg cit), Datenauswahl (Art 10 leg cit), technische Dokumentation (Art 11 leg cit), Aufzeichnungspflichten (Art 12 leg cit), Transparenzpflichten (Art 13 leg cit), menschliche Aufsicht (Art 14 leg cit), Sicherheitsanforderungen (Art 15 leg cit); Stelmasczyk/Wosgien, Die Digitalisierungsrichtlinie 2.0, EuZW 2023, 550 (553).

<sup>25</sup> Vgl von Lewinski in Wolff/Brink/v. Ungern-Sternberg (Hrsg), BeckOK Datenschutzrecht<sup>45</sup> (1. 8. 2023) Art 22 Rz 13a, gemäß welchem „künstliche Intelligenz“ die für die automatisierte Entscheidungsfindung geforderte Komplexitätsschwelle erreicht.

<sup>26</sup> Buchner in Kühling/Buchner (Hrsg), DS-GVO<sup>3</sup> (2020) Art 22 Rz 15.

<sup>27</sup> Dies selbstredend nur dann, wenn die berufsrechtliche Zulässigkeit gegeben ist. Vgl allgemein zur rechtlichen Wirkung sowie erheblichen Beeinträchtigung in ähnlicher Weise von Lewinski in BeckOK Datenschutzrecht (FN 25) Art 22 Rz 28 ff, 37; Buchner in DS-GVO (FN 26) Art 22 Rz 26a.

<sup>28</sup> IA 1191/A, 27. GP 18.  
<sup>29</sup> Zur Problematik unbestimmter Gesetzesbegriffe im Hinblick auf die Sanktionierung bei deren Nichteinhaltung s Lehner/Vitek in RAO (FN 2) § 8a Rz 7, 43, 53.

## Geldwäscheprävention

walt in § 8a Abs 2 RAO im Rahmen der kanzleibezogenen Compliance die Verpflichtung zur Einführung „angemessener und geeigneter Strategien und Verfahren“ zur Erfüllung seiner Sorgfaltspflichten auferlegt. Nach Auffassung des ÖRAK impliziert dies die Einführung „standardisierter Verfahren“ zur Verhinderung einer bloß anlassfallbezogenen („ad hoc“) Compliance. Gleichermaßen verpflichtet § 8a Abs 4 RAO den Rechtsanwalt zur Einführung eines dynamischen<sup>30</sup> Risikomanagementsystems, um die PEP-Eigenschaft einer Person feststellen zu können. Im Falle des Vorliegens von Kanzleiniederlassungen neben der Hauptniederlassung ist der Rechtsanwalt (auch) zur Einrichtung und Aufrechterhaltung von „Datenschutzstrategien“ sowie „Strategien und Verfahren für den internen Informationsaustausch“ verpflichtet (§ 8a Abs 5 RAO).

Vereinzelte enthalten die §§ 8a ff RAO jedoch auch Hinweise auf technische Verfahren bzw. „best practices“, deren Verwendung entweder erlaubt bzw. angeregt wird oder die verpflichtend sind. So wird im Rahmen des KYC die Identitätsfeststellung der Partei anhand von „gesetzlich vorgesehenen oder anerkannten sicheren“ elektronischen Verfahren und Mitteln aus der Ferne sowie Identifizierungsmitteln, die von einem „notifizierten elektronischen Identifizierungssystem“ mit dem Sicherheitsniveau „substantiell“ oder „hoch“ nach Maßgabe der eIDAS-VO<sup>31</sup> ausgestellt wurden, erlaubt (§ 8b Abs 2 RAO). Ebenso wird, bezogen auf die Identifizierungspflicht des wirtschaftlichen Eigentümers, auf das WiEReG<sup>32</sup> sowie wesensgleiche Register in anderen Mitgliedstaaten oder bestimmten<sup>33</sup> Drittstaaten Bezug genommen (§ 8b Abs 4, 4a RAO). § 8c Abs 1 RAO enthält die Verpflichtung des Rechtsanwalts zur Übermittlung der Verdachtsmeldung in einem „geläufigen elektronischen Format“ (XML)<sup>34</sup> unter Verwendung eines sicheren Kommunikationskanals, der von der Geldwäschemeldestelle festgelegt wurde (goAML).<sup>35</sup> Zudem muss der Rechtsanwalt im Rahmen seiner Auskunftspflicht über Systeme verfügen, die eine sichere und vertrauliche Kommunikation mit der Geldwäschemeldestelle ermöglichen (§ 9 Abs 6 RAO).

Aus technischer Perspektive ergibt sich sohin bei den zu implementierenden Compliance-Maßnahmen ein zweistufiges System: Soweit nach Maßgabe der gesetzlichen Bestimmungen, allenfalls ergänzt durch Präzisierungen der Geldwäschemeldestelle, technische Eckpfeiler vorgegeben werden, sind diese vom Rechtsanwalt umzusetzen. Darüber hinaus wird er bei der Umsetzung wohl insoweit Freiheit genießen, sofern die jeweiligen gesetzlichen Anforderungen wirksam erreicht werden können (also zB die im Rahmen des § 8a Abs 2 RAO gewählten Strategien und Maßnahmen des Rechtsanwalts „angemessen“ und „geeignet“ sind). Dem steht die Einbindung von Automatisierungsstrategien bzw. die Verwendung fortgeschrittener Technologien grundsätzlich nicht entgegen, sofern die sonstigen rechtlichen, insbesondere datenschutzrechtlichen, Rahmenbedingungen eingehalten werden.

## 2. Datenschutzrechtlicher Rahmen

Die Verarbeitung personenbezogener Daten hat stets in Einklang mit den Bestimmungen der DSGVO<sup>36</sup>, flankiert von den einschlägigen unionalen<sup>37</sup> sowie nationalen datenschutzrechtlichen Vorschriften, zu erfolgen. Zwei dieser Verpflichtungen werden in § 9 Abs 5 RAO näher spezifiziert.

In § 9 Abs 5 Satz 1 RAO ist zunächst die datenschutzrechtliche Informationspflicht geregelt: Demgemäß hat der Rechtsanwalt einer neuen Partei die nach den Art 13f DSGVO erforderlichen Informationen vor Begründung der Geschäftsbeziehung bzw. Durchführung der Transaktion bereitzustellen. Im Falle des Vorliegens eines Geschäfts nach § 8a Abs 1 RAO ist zusätzlich<sup>38</sup> ein „allgemeine[r] Hinweis zu den rechtlichen Pflichten des Rechtsanwalts“ nach Maßgabe der RAO bei der Verarbeitung personenbezogener Daten zur Verhinderung von ML und FT anzufügen. Mangels gegenläutender Bestimmung umfasst die zu erteilende (datenschutzrechtliche) Information sämtliche Pflichtangaben nach den Art 13 bzw. 14 DSGVO,<sup>39</sup> sohin auch die Information, ob eine automatisierte Entscheidungsfindung einschließlich Profiling iSd Art 22 Abs 1 und 4 DSGVO vorliegt, und „zumindes in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“. Möchte der Rechtsanwalt also im Bereich der Verhinderung von ML und FT ein solches System zur automatisierten Entscheidungsfindung einsetzen, so hat er die Partei hierüber im Vorhinein in Kenntnis zu setzen. Ob die Informationspflicht auch Details zum konkreten Algorithmus umfassen muss, ist umstritten,<sup>40</sup> wobei einerseits die Offenlegung der

<sup>30</sup> Bezogen auf die konkrete Geschäftstätigkeit, Art und Größe der Kanzlei.

<sup>31</sup> Verordnung (EU) Nr 910/2014 des Europäischen Parlaments und des Rates vom 23. 7. 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG idF der Berichtigung ABl L 155 vom 14. 6. 2016, 44.

<sup>32</sup> Wirtschaftliche Eigentümer Registergesetz (WiEReG), BGBl I 2017/136 idF BGBl I 2023/97.

<sup>33</sup> § 8b Abs 4 S 2 RAO.

<sup>34</sup> Extensible Markup Language. Die A-FIU regte in Schulungen und Vorträgen die Verwendung des strukturierten XML-Dateiformats zur Einbringung von Verdachtsmeldungen an, s Bundesministerium für Inneres, Lagebericht Geldwäsche 2022, 57.

<sup>35</sup> Eine Beschreibung zur Nutzung von goAML wird vom Bundesministerium für Inneres unter <https://bundeskriminalamt.at/308/start.aspx> bereitgestellt (abgefragt 20. 10. 2023).

<sup>36</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO), ABl L 119, 1 idF ABl L 74 vom 4. 3. 2021.

<sup>37</sup> Vgl Art 41 ff Richtlinie (EU) 2015/849 vom 20. 5. 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl L 141, 73 vom 5. 6. 2015 idF ABl L 344, 155 vom 27. 12. 2019.

<sup>38</sup> Lehner in RAO (FN 2) § 9 Rz 69.

<sup>39</sup> Vgl die Auflistung zu Art 13 bei Lehner in RAO (FN 2) § 9 Rz 70.

<sup>40</sup> Für einen Überblick über den Meinungsstand s Paal/Hennemann in Paal/Pauly (Hrsg), DS-GVO<sup>3</sup> (2021) Art 13 Rz 31 b; auf die Unklarheit der gesetzlichen Bestimmungen jüngst auch hinweisend Schmidt-Wudy in BeckOK Datenschutzrecht (FN 25) Art 15 Rz 78.

Funktionsweise des konkret eingesetzten Algorithmus,<sup>41</sup> andererseits – auch unter Berücksichtigung des Wissensstands der Partei sowie der Wahrung von Geschäfts- und Betriebsgeheimnissen – die Darlegung der „*allgemeinen Funktionsweise*“ vertreten wird.<sup>42</sup> Ein weiteres Problem ergibt sich zudem aus dem Telos der Bestimmungen zur Verhinderung von ML und FT selbst: Wird das vom Rechtsanwalt eingesetzte System zur automatisierten Entscheidungsfindung im Rahmen der Informationspflicht zu extensiv erklärt und insbesondere auf die maßgeblichen Grundlagen und Parameter zur Entscheidungsfindung eingegangen, könnten einer schlechtgläubigen Partei mögliche Umgehungswege aufgezeigt werden. Eine entsprechende gesetzliche Einschränkung der Auskunftspflicht durch den Gesetzgeber *de lege ferenda* zur Eindämmung dieses Risikos wäre sohin wünschenswert.<sup>43</sup>

In § 9 Abs 5 S 3 RAO wird geregelt, dass die Verarbeitung personenbezogener Daten auf Grundlage der RAO zu Zwecken der Verhinderung von ML und FT als „*Angelegenheit von öffentlichem Interesse gemäß der DSGVO*“ anzusehen ist.<sup>44</sup> Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Rechtsanwälte zum vorgenannten Zweck ist sohin – auch unter dem Gesichtspunkt der Erfüllung der berufsrechtlichen Verpflichtungen iZm ML und FT, denen der Rechtsanwalt unterliegt – Art 6 Abs 1 lit c DSGVO iVm § 9 Abs 5 RAO.<sup>45</sup> Zu hinterfragen ist jedoch die Reichweite der Rechtsgrundlage hinsichtlich Datenverarbeitungen unter Zugrundelegung fortgeschrittener Technologien wie bspw künstlicher Intelligenz: Eine Datenverarbeitung, die über das gesetzlich festgeschriebene Ziel „*hinausschießt*“, ist mit Art 6 Abs 1 lit c DSGVO nicht in Einklang zu bringen.<sup>46</sup> Damit ist insb bei weit bzw abstrakt gefassten Pflichten die Frage der Erforderlichkeit der Datenverarbeitung zur Zweckerreichung zu stellen.<sup>47</sup>

Daraus lässt sich folgende Überlegung ableiten: Wenn es im Bereich der Bekämpfung von ML und FT (absolut) erforderlich ist, Strategien bzw Verfahren einzusetzen, die Datenverarbeitungsprozesse mit bestimmter Komplexität unter Heranziehung fortgeschrittener Technologien zum Gegenstand haben, um der anwaltlichen Sorgfaltspflicht (bspw nach § 8a Abs 2 RAO) nachzukommen, dann soll deren Einsatz auch datenschutzrechtlich zulässig sein. Zu differenzieren ist dabei stets zwischen Systemen, die Entscheidungen zur weiteren menschlichen Entscheidung lediglich vorbereiten, und jenen, die in den Anwendungsbereich des Art 22 DSGVO fallen („*vollautonome Systeme*“). Inwieweit jedoch „*vollautonome Systeme*“ zur Entscheidungsfindung jedenfalls aus Perspektive des Datenschutzes tatsächlich zulässig sind, muss offengelassen werden.<sup>48</sup> Jedes einzusetzende System erfordert daher eine tiefgreifende Analyse, ob ein solcher Einsatz aus datenschutzrechtlichen Gesichtspunkten zulässig ist.

Unabhängig davon sind auch die weiteren datenschutzrechtlichen Anforderungen zu prüfen, insbesondere, ob durch den beabsichtigten Einsatz des Systems die Grund-

sätze der Datenverarbeitung iSd Art 5 Abs 1 DSGVO eingehalten werden und eine Datenschutzfolgenabschätzung durchgeführt werden muss.<sup>49</sup>

#### IV. AUTOMATISIERUNG BZW FORTSCHRITTLICHE TECHNOLOGIEN IM KANZLEIINTERNEN COMPLIANCE-SYSTEM

In Einklang mit § 8a Abs 2 RAO obliegt dem Rechtsanwalt selbst die Auswahl der zur Erfüllung seiner Compliance-Pflichten angemessenen und geeigneten Strategien und Verfahren; er trifft sohin letztlich auch die Entscheidung, welches technische System er in den Kanzleibetrieb integriert.<sup>50</sup> Ein zeitgemäßes System sollte nach Auffassung des Autors jedoch nachstehende Kriterien erfüllen:

Zunächst sollte das eingesetzte Compliance-System über eine tiefe Integration in die bestehende Aktenverwaltungssoftware („*Hauptsystem*“) verfügen, wobei dies durch ent-

<sup>41</sup> Bäcker in DS-GVO (FN 26) Art 13 Rz 54.  
<sup>42</sup> Wiederum Paal/Hennemann in DS-GVO (FN 40)<sup>3</sup> Art 13 Rz 31 b f.  
<sup>43</sup> Eine solche ist dem Gesetzgeber grundsätzlich nach Art 23 Abs 1 lit d bzw e DSGVO möglich. Zu berücksichtigen ist jedoch die Vorgabe in Art 41 Abs 3 S 1 der Richtlinie (EU) 2015/849 idF ABl L 344, 155 vom 27. 12. 2019, in welcher eine solche Einschränkung der Informationspflicht nicht vorgesehen ist (dies jedoch unter Bezugnahme auf Art 10 der mittlerweile nicht mehr in Geltung stehenden Richtlinie [EU] 95/46/EU, in welchem die Informationserteilung zur automatisierten Entscheidungsfindung noch unberücksichtigt blieb).  
<sup>44</sup> Vgl auch die zugrunde liegende Bestimmung gemäß Art 43 Richtlinie (EU) 2015/849 idF ABl L 344, 155 vom 27. 12. 2019.  
<sup>45</sup> Dies unter Wahrung der Voraussetzungen in Art 6 Abs 3 DSGVO: So wird die Rechtsgrundlage sowohl durch Unionsrecht (Art 43 Richtlinie [EU] 2015/849 idF ABl L 344, 155 vom 27. 12. 2019) als auch durch nationales Recht (§ 9 Abs 5 RAO) festgelegt, wobei der Zweck der Verarbeitung (Verhinderung von ML und FT) in der jeweiligen Rechtsmaterie als eine „*Angelegenheit von öffentlichem Interesse*“ definiert ist.  
<sup>46</sup> Buchner/Petri in DS-GVO (FN 26) Art 6 Rz 81.  
<sup>47</sup> Albers/Veit in BeckOK Datenschutzrecht (FN 25) Art 6 Rz 50. Ein Abgehen des Verantwortlichen von der Verpflichtung zum „*self assessment*“, ob die gewählten Maßnahmen erforderlich sind, ist auch durch die künftige Geldwäsherverordnung nicht zu erwarten. Wengleich diese eine explizite Rechtsgrundlage zur Verarbeitung personenbezogener Daten (einschließlich jener nach Art 9 Abs 1 sowie Art 10 DSGVO) enthält, wird bei der Zulässigkeit deren Inanspruchnahme auf die „*unbedingte Erforderlichkeit*“ der Verhinderung von ML und FT abgestellt, s Art 55 Abs 1, 3 des Vorschlags der Europäischen Kommission für eine Verordnung zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, COM(2021) 420 final vom 20. 7. 2021; vgl zur datenschutzrechtlichen Rechtsgrundlage nach Art 55 des Verordnungsvorschlags vertiefend Seehafer, Digitalisierung für die Geldwäscheprävention nutzen: Combined Data Analytics im Transaktionsmonitoring (Teil II), dtGWuR 2022, 135 (135).  
<sup>48</sup> Mit Art 22 DSGVO wird ein grundsätzliches Verbot der automatisierten Entscheidungsfindung im Einzelfall einschließlich Profiling statuiert, von welchem Ausnahmen bestehen. Die (generalisierte) Rechtsgrundlage bzw Klarstellung nach § 9 Abs 5 RAO reicht nach Auffassung des Autors nicht, um einen Ausnahmetatbestand nach Art 22 Abs 2 lit b DSGVO zu begründen, da diese gesetzliche Bestimmung keine dezidierten „*angemessene[n] Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person*“ enthält, deren Angabe gemäß der Öffnungsklausel der DSGVO erforderlich wäre. Fraglich ist hingegen, ob der Ausnahmetatbestand nach lit a leg cit erfüllt ist; dies könnte wohl dann argumentiert werden, wenn die vorzuschaltende Prüfung des Vorliegens von Geldwäscherei oder Terrorismusfinanzierung (bzw das Negativergebnis) für den Abschluss des Mandatsvertrags zwingend erforderlich ist, sie sohin „*in unmittelbarem Zusammenhang*“ mit dem Mandatsvertrag steht, vgl auch Buchner in DS-GVO (FN 26) Art 22 Rz 30.  
<sup>49</sup> Insb beim Einsatz von „*künstlicher Intelligenz*“ ist eine solche indiziert, vgl § 2 Abs 2 Z 4 der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl II 2018/278; vgl auch zu § 7a FM-GwG IA 1191/A, 27. GP 18.  
<sup>50</sup> Lehner/Vitek in RAO (FN 2) § 8a Rz 17.

## Geldwäscheprävention

sprechende Plugins sichergestellt werden kann.<sup>51</sup> Insofern muss eine Kompatibilität zwischen Compliance-System und Hauptsystem gewährleistet sein. Das System sollte modular an die Bedürfnisse der jeweiligen Kanzlei, die im Rahmen der allgemeinen Risikoanalyse iSd § 8a Abs 3 RAO ermittelt wurden, angepasst werden können und standardisierte Verfahren bereitstellen.<sup>52</sup>

Das Compliance-System sollte in technischer Hinsicht so ausgestaltet sein, dass dem Rechtsanwalt in höchstmöglicher Weise administrative Arbeit abgenommen wird. Erhebliches Automatisierungspotenzial ist daher im Bereich der mandatsbezogenen Compliance gegeben, wobei die nachfolgenden Vorschläge stets unter der Voraussetzung technischer Machbarkeit stehen. So könnte die nach § 8b Abs 4, 4a RAO vorgesehene Einsicht in das WiEReG (bzw in ein anderes Register in einem Mitgliedstaat oder einem Drittstaat) vollautomatisiert durch entsprechende Verknüpfung mit den jeweiligen Diensteanbietern über Application Programming Interfaces (APIs)<sup>53</sup> realisiert werden. Gleiches gilt für die (unterstützende) Überprüfung, ob es sich bei der Partei um eine PEP handelt (§ 8f Abs 1 RAO). Soweit vom Rechtsanwalt und/oder der Partei Fragebögen auszufüllen sind, könnten die Links zu den Webformularen dazu automatisiert mittels E-Mail an die hinterlegten Mailadressen versandt werden; eine Unterfertigung durch die Partei kann dabei durch eine qualifizierte elektronische Signatur nach der eIDAS-VO erfolgen. Zusätzlich könnte zur Unterstützung der Verpflichtung des Rechtsanwalts, die Geschäftsbeziehung laufend zu überwachen (§ 8b Abs 6 RAO), abgefragt werden, ob sich die jeweiligen Informationen der Partei (zB Firmensitz oder Eigentumsverhältnisse) mittlerweile geändert haben.<sup>54</sup> Im Rahmen der Dokumentations- bzw Aufbewahrungspflicht nach § 8b Abs 5 und 6 RAO könnte das System unterstützend die jeweiligen Dokumente zusammenstellen bzw organisieren. Ebenso sollte das System die Erstattung von Verdachtsmeldungen an die Geldwäschemeldestelle (§ 8c Abs 1 RAO) mittels API unterstützen, samt Implementierung einer Akt-Bearbeitungssperre in den Fällen des § 8c Abs 2, 3 RAO.

Schließlich sollte das System ein anonymes Whistleblowing gemäß § 9 Abs 8 RAO bereitstellen.

In Bezug auf die Implementierung „intelligenter“ Datenverarbeitungsprozesse lohnt sich ein Blick auf die Vorschläge der FATF: Diese regt insbesondere im Bereich der Überwachung der Geschäftsbeziehung den Einsatz von Machine Learning an.<sup>55</sup> Zusätzlich können spezifisch trainierte Large Language Models (LLM) eingesetzt werden, um den Rechtsanwalt bei der Evaluierung eines komplexen Sachverhalts – bspw bezogen auf die Frage, ob das jeweilige Geschäft ein geldwäschegeneigtes Geschäft iSd § 8a Abs 1 RAO ist, oder ob die vereinfachte Sorgfaltspflicht iSd § 8e RAO zur Anwendung kommt – zu unterstützen.

### V. SCHLUSSBEMERKUNGEN

Automatismen sowie fortschrittliche Technologien wie beispielsweise künstliche Intelligenz sind geeignet, den Rechtsanwalt bei seinen gesetzlichen Compliance-Pflichten zu unterstützen. Stets zu beachten ist dabei die berufs- und datenschutzrechtliche Zulässigkeit der zu implementierenden Systeme. Hervorzuheben ist, dass Normadressat sowohl für die kanzlei- als auch mandatsbezogenen Sorgfaltspflichten der Rechtsanwalt selbst ist. „Intelligente“ Systeme können ihn dabei demgemäß (bloß) unterstützen, er darf jedoch das Heft der Pflichtenerfüllung nicht aus der Hand geben.

<sup>51</sup> Der Vorteil einer solchen Verschränkung liegt darin, dass die gesamte Compliance bezogen auf das Frontend (idealerweise) innerhalb eines einzigen genutzten Systems abgedeckt werden kann und eine „Zersplitterung der Nutzung“ über mehrere dedizierte Insellösungen hinweg vermieden wird.

<sup>52</sup> Vgl den Hinweis auf das „planmäßige“ und „organisatorisch verfestigte“ Vorgehen von *Lehner/Vitek* in RAO (FN 2) § 8a Rz 17 mwN *Wöß*, Geldwäscherei 5.0, 12.

<sup>53</sup> Programmierschnittstellen.

<sup>54</sup> Eine diesbezügliche Verpflichtung zur Gewährleistung der Datenrichtigkeit (bzw -aktualität) ergibt sich zusätzlich aus dem Datenschutzrecht (Grundsatz der Datenrichtigkeit, Art 5 Abs 1 lit d DSGVO).

<sup>55</sup> *FATF*, Opportunities and Challenges (FN 10), Box 8.