**Berichts-Motion von Esther Monney und Thomas Werner
betreffend künstliche Intelligenz (KI) im Dienste des Kantons Zug: Rechtliche Grundlagen für den Einsatz in Verwaltung, Justiz und Polizei (Vorlage Nr. 3872.1 - 18020)
Postulat von Joëlle Gautier, Jill Nussbaumer, Etienne Schumpf, Alex Haslimann und Michael Felber
betreffend Schaffung von Grundlagen für die erfolgreiche Anwendung von KI-Modellen im öffentlichen Sektor (Vorlage Nr. 3896.1 - 18086)**

Bericht und Antrag des Regierungsrats
vom 9. Juni 2026

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Esther Monney und Thomas Werner haben am 30. Januar 2025 eine Berichts-Motion betreffend künstliche Intelligenz (KI) im Dienste des Kantons Zug: Rechtliche Grundlagen für den Einsatz in Verwaltung, Justiz und Polizei eingereicht (Vorlage Nr. 3872.1 - 18020). Joëlle Gautier, Jill Nussbaumer, Etienne Schumpf, Alex Haslimann und Michael Felber haben am 15. März 2025 ein Postulat betreffend Schaffung von Grundlagen für die erfolgreiche Anwendung von KI-Modellen im öffentlichen Sektor eingereicht (Vorlage Nr. 3896.1 - 18086). Der Kantonsrat hat die Berichts-Motion am 20. Februar 2025 und das Postulat am 10. April 2025 überwiesen. Wir unterbreiten Ihnen hierzu Bericht und Antrag wie folgt:

1. Einleitende Bemerkungen

Der Einsatz von künstlicher Intelligenz (KI) in Verwaltung und Justiz wirft rechtliche, technische und organisatorischen Fragen auf und verlangt eine Betrachtung der internationalen, nationalen und kantonalen Entwicklungen. Der Bericht stellt die massgeblichen rechtlichen Rahmenbedingungen, mögliche Anwendungsfelder in der kantonalen Verwaltung und Justiz sowie die damit verbundenen Chancen und Herausforderungen dar. Aufgrund der inhaltlichen und rechtlichen Komplexität sowie der dynamischen technologischen Entwicklung ist eine differenzierte Beurteilung erforderlich. Die Polizei wird nicht gesondert behandelt, da sie organisatorisch Teil der kantonalen Verwaltung ist und der Sicherheitsdirektion untersteht.

2. In Kürze

KI kann staatliche Stellen bei der Verarbeitung grosser Datenmengen, bei wiederkehrenden administrativen Tätigkeiten, bei der strukturierten Aufbereitung von Informationen und damit bei Effizienzsteigerung und Entlastung der Mitarbeitenden unterstützen. Gleichzeitig stellen sich Fragen zu Grundrechten, Transparenz, Datenschutz, Informationssicherheit und Nachvollziehbarkeit staatlicher Entscheidungen. Voraussetzung für jeden Einsatz ist die Einhaltung rechtsstaatlicher Grundsätze sowie der verfahrens- und datenschutzrechtlichen Vorgaben.

International sind die KI-Konvention des Europarats und der AI Act der Europäischen Union zentral. Der AI Act schafft innerhalb der EU einen unmittelbar geltenden Rechtsrahmen für Entwicklung und Einsatz von KI-Systemen. Die KI-Konvention ist demgegenüber ein völkerrechtliches Rahmenabkommen, das innerstaatlich umzusetzen ist. Für die Schweiz gilt der AI Act nicht unmittelbar, kann aber relevant werden, wenn KI-Systeme aus der Schweiz im EU-Raum eingesetzt werden. Die Schweiz hat die KI-Konvention ratifiziert. Der Bundesrat beabsichtigt, sie bis Ende 2026 in das Schweizer Recht zu überführen. Daraus können sich Auswirkungen auf kantonaler Ebene ergeben. Parallel laufen koordinierte Arbeiten der Kantone unter Einbezug der Konferenz der Kantonsregierungen (KdK), deren Ergebnisse abzuwarten sind.

Der Regierungsrat gelangt zum Schluss, dass bereits heute technologieneutrale Rechtsgrundlagen auf Bundes- und Kantonsebene bestehen, die den Einsatz von KI grundsätzlich ermöglichen, sofern die geltenden Vorgaben eingehalten werden. Ein unmittelbarer gesetzgeberischer Handlungsbedarf für den Kanton Zug besteht derzeit nicht. Zweckmässig ist jedoch mehr

Transparenz über den Einsatz von KI in der Verwaltung. Vorgesehen ist eine Übersicht über die eingesetzten KI-Anwendungen in der kantonalen Verwaltung, welche Einsatzbereiche und Zwecke sichtbar macht, ohne sicherheitsrelevante oder besonders schützenswerte Informationen offenzulegen. Dies stärkt Nachvollziehbarkeit und Vertrauen in einen verantwortungsvollen Umgang mit neuen Technologien.

3. Berichts-Motion von Esther Monney und Thomas Werner betreffend künstliche Intelligenz (KI) im Dienste des Kantons Zug: Rechtliche Grundlagen für den Einsatz in Verwaltung, Justiz und Polizei (# 3872)

Gemäss § 43 Abs. 1 des Kantonsratsbeschlusses über die Geschäftsordnung des Kantonsrats (GO KR) vom 28. August 2014 (BGS 141.1) sind Motionen Anträge, durch deren Erheblicherklärung der Regierungsrat, die Gerichte oder eine Kommission des Kantonsrats beauftragt werden, einen Verfassungs-, Gesetzes- oder Beschlussentwurf oder einen Bericht in einer kantonalen Angelegenheit mit Lösungsvorschlägen vorzulegen. Letzteres ist die Berichts-Motion. Sie dient einer Grundsatzdiskussion, dem Aufzeigen von Lösungsmöglichkeiten und der Vorbereitung einer späteren Motion. Das Motionsbegehren beinhaltet die Erstellung eines Berichts mit klar umrissener Thematik und Lösungsvorschlägen, nicht aber einen Erlassentwurf[1].

Grundsätzlich gilt auch für Berichts-Motionen das zweistufige Verfahren nach § 45 und § 48 GO KR: Zunächst beantragt der Regierungsrat innert einem Jahr seit Überweisung, ob die Motion erheblich zu erklären und ein Bericht zu erstellen sei (nach § 45 Abs. 3 GO KR[2]). Bei Erheblicherklärung legt er den Bericht innert drei Jahren vor. Wird die Motion nicht erheblich erklärt, entfällt der Bericht. Der Bericht samt Lösungsvorschlägen kann beraten werden, wird aber nur zur Kenntnis genommen; materielle Beschlüsse erfolgen nicht. Auf seiner Grundlage kann eine weitere Motion eingereicht werden. Nach § 49 GO KR ist ausnahmsweise ein einstufiges Verfahren möglich, bei dem Behandlung und Erledigung im selben Bericht und Antrag erfolgen. Der Regierungsrat erachtet dies im vorliegenden Fall als sachgerecht und legt dem Kantonsrat gleichzeitig Bericht und Antrag zur Erledigung vor.

---

1 Tino Jorio, Geschäftsordnungen des Regierungsrats und des Kantonsrats des Kantons Zug, Zürich 2015, Rz. 644.
2 Tino Jorio, a.a.O., Rz. 644.

3.1. Begriff der künstlichen Intelligenz (KI)

Eine allgemeingültige Definition von KI besteht nicht. In der Rechtssetzung wird ein KI-System häufig als maschinenbasiertes System verstanden, das aus übermittelten Eingaben explizite oder implizite Ziele ableitet und daraus Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generiert, die physische oder virtuelle Umgebungen beeinflussen können. KI-Systeme unterscheiden sich in Autonomiegrad und Anpassungsfähigkeit nach Inbetriebnahme. Vereinfacht imitiert KI menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität. KI-Technologien nehmen Signale wahr, analysieren diese und führen gestützt darauf Aktionen aus, etwa Benachrichtigungen, Empfehlungen, Prognosen oder Entscheide. Diese Aktionen können einen endgültigen Entscheid bilden (Vollautomation) oder einer natürlichen Person als Entscheidgrundlage dienen (Teilautomation). KI ist als Grundlagentechnologie wesentlicher Bestandteil der Digitalisierung von Staat, Wirtschaft und Gesellschaft.

3.2. KI-Konvention und AI Act

Am 17. Mai 2024 verabschiedete das Ministerkomitee des Europarats die Rahmenkonvention über künstliche Intelligenz und Menschrechte, Demokratie und Rechtsstaatlichkeit» (sog. «KI-Konvention»)[3]. Sie ist das erste globale, zwischenstaatlich verbindliche Abkommen zur Regulierung von KI und steht weltweit zur Unterzeichnung offen[4]. Praktisch gleichzeitig trat am 1. August 2024 die EU-KI-Verordnung (sog. «AI Act»)[5] in Kraft, sie ist ab dem 2. August 2026 mit gewissen Ausnahmen in den EU-Mitgliedstaaten unmittelbar anwendbar[6]. Beide Regelwerke reagieren auf Chancen für Innovation und Wirtschaftswachstum sowie auf erhebliche Risiken für Menschenrechte, Demokratie, Rechtsstaatlichkeit, Gesundheit, Sicherheit und Grundrechte, namentlich Überwachung, Diskriminierung und andere gesellschaftliche Schäden.

3.2.1. Rahmenkonvention des Europarates über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit (KI-Konvention)

Die KI-Konvention setzt einen gemeinsamen Mindeststandard. Sie soll über den gesamten Lebenszyklus von KI-Systemen den Schutz von Menschenrechten, die Integrität demokratischer Prozesse und den Respekt der Rechtsstaatlichkeit gewährleisten[7]. Anlass sind insbesondere Risiken von Missbrauch, Diskriminierung, unrechtmässige Überwachung und Einschränkungen individueller Autonomie von der Entwicklung bis zur Ausserbetriebnahme[8].

Die Konvention enthält Grundprinzipien für den Umgang mit KI, verpflichtet zur Schaffung oder Aufrechterhaltung von Verfahrensgarantien und Rechtsmitteln und verlangt eine Abschätzung von Risiken sowie nachteiligen Auswirkungen. Im Unterschied zum AI Act enthält sie keine konkreten Verbote von KI-Systemen mit unannehmbaren Risiken, sondern verpflichtet die Vertragsstaaten zur Prüfung risikobasierter Massnahmen. Ihr Anwendungsbereich erfasst KI-Aktivitäten öffentlicher Stellen und Privater, die im Auftrag der öffentlichen Verwaltung handeln.

---

[3] Rahmenkonvention des Europarates über künstliche Intelligenz und Menschrechte, Demokratie und Rechtsstaatlichkeit vom 17. Mai 2024 (nachfolgend: KI-Konvention; https://www.coe.int/de/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence und CM(2024)52-fi https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680afb11f%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}nal; besucht am 5. März 2026).

[4] BAKOM, Auslegeordnung zur Regulierung von künstlicher Intelligenz, Bericht an den Bundesrat vom 12. Dezember 2025, S. 7 (nachfolgend: BAKOM, Auslegeordnung).

[5] EU-Verordnung 2024/1689 vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (nachfolgend: AI Act; https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689; besucht am 5. März 2026).

[6] Art. 113 des AI Act sieht gewisse Ausnahmen vor: Danach treten Kapitel I und II des AI Act bereits ab dem 2. Februar 2025 in Kraft, andere Bestimmungen gelten ab dem 2. August 2025 und Art. 6 Abs. 1 tritt mit den entsprechenden Pflichten erst am 2. August 2027 in Kraft.

[7] BAKOM, Auslegeordnung, S. 7 f.

[8] Siehe hierzu auch: Susanne Kuster/Jonas Zaugg, Die Schweiz sucht bei der KI-Regulierung den Mittelweg, in: Die Volkswirtschaft vom 15. April 2025 (https://dievolkswirtschaft.ch/de/2025/04/die-schweiz-sucht-bei-der-ki-regulierung-den-mittelweg/; besucht am 5. März 2026).

Risiken im rein privaten Sektor sind im konventionsgemässen Rahmen zu adressieren. Die Vertragsstaaten legen gegenüber dem Generalsekretär des Europarats offen, wie sie den privaten Sektor einbeziehen. Ausgenommen sind Landesverteidigung, mit Ausnahmen Forschung und Entwicklung sowie nationale Sicherheit, sofern diese nicht unterstellt wird[9, 10].

Zentrale Vertragspunkte sind der Schutz der Menschenrechte (Art. 4), die Integrität demokratischer Prozesse sowie Achtung der Rechtsstaatlichkeit (Art. 5) sowie die Umsetzung grundlegenden Prinzipien insnationale Recht (Art. 6):

- Achtung der Menschenwürde und Gewährleistung der individuellen Autonomie (Art. 7),
- Gewährleistung von Transparenz- und Aufsichtsanforderungen (Art. 8),
- Gewährleistung der Rechenschaftspflicht und Verantwortung für nachteilige Auswirkungen auf die Menschenrechte, die Demokratie und die Rechtsstaatlichkeit (Art. 9),
- Gewährleistung der Gleichstellung und Nichtdiskriminierung (Art. 10),
- Schutz der Privatsphäre und von personenbezogenen Daten (Art. 11),
- Förderung der Zuverlässigkeit von KI-Systemen und des Vertrauens in deren Ergebnisse (Art. 12) und
- Förderung sicherer Innovationen durch Schaffung kontrollierter Umgebungen für die Entwicklung, Erprobung und Prüfung künstlicher Intelligenzsysteme unter der Aufsicht der zuständigen Behörden (Art. 13).

Hinzu kommen zugängliche und wirksame Rechtsbehelfe bei Menschenrechtsverletzungen, Informations-, Dokumentations- und Editionspflichten (Art. 14), Verfahrensgarantien bei erheblichen Auswirkungen auf die Ausübung von Menschenrechten (Art. 15) sowie Anforderungen an Bewertung und Minderung von Risiken. Für die Umsetzung verlangt die Konvention zudem Vorkehrungen zur Nichtdiskriminierung (Art. 17), zum Schutz von Kindern und Menschen mit Behinderungen (Art. 18), zu Diskussionen und öffentlichen Konsultationen (Art. 19), zur Förderung digitaler Kompetenzen (Art. 20) und zur Sicherung beziehungsweise Anhebung bestehender Grundrechtsstandards (Art. 21–22).

Die Konvention ist nicht self-executing und richtet sich primär an die Vertragsstaaten. Für die Schweiz folgt aus der Ratifikation vom 27. März 2025 die Pflicht, geeignete Gesetzgebungs-, Verwaltungs- oder sonstige Massnahmen zu prüfen und umzusetzen. Das Bundesamt für Justiz hält in seiner rechtlichen Basisanalyse[11] vom 31. August 2024 fest, dass die allgemein formulierten Regeln und Grundsätze in innerstaatliches Recht zu überführen sind. Gestützt auf Art. 5 Abs. 4 der Bundesverfassung der Schweizerischen Eidgenossenschaft (BV) vom 18. April 1999 (SR 101) ist zu prüfen, welche Pflichten aus der Konvention vom Bund respektive von den Kantonen umzusetzen haben[12].

3.2.2. EU-Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (AI Act)

Der AI Act setzt einen einheitlichen, unmittelbar geltenden Rechtsrahmen für Entwicklung, Inverkehrbringen, Inbetriebnahme und Verwendung von KI-Systemen in der EU. KI-Systeme sollen während ihres Lebenszyklus sicher sein, den EU-Normen entsprechen, grenzüberschreitend frei verkehren und den EU-Binnenmarkt nicht fragmentieren. Gefördert werden menschenzentrierte, diskriminierungsfreie und vertrauenswürdige KI sowie ein hohes Schutzniveau für Gesundheit, Sicherheit und Grundrechte.

---

9 BAKOM, Auslegeordnung, S. 8.
10 BAKOM, Auslegeordnung, S. 8.
11 Bundesamt für Justiz (BJ), Rechtliche Basisanalyse im Rahmen der Auslegeordnung zu den Regulierungsansätzen im Bereich künstliche Intelligenz vom 31. August 2024 (nachfolgend: BJ, Rechtliche Basisanalyse).
12 BJ, Rechtliche Basisanalyse, S. 13–15. Die Rechtliche Basisanalyse enthält in Kapitel 4, S. 13 – 88., detaillierte Ausführungen zur KI-Konvention und deren Auswirkungen auf das Schweizer Recht.

Der Anwendungsbereich von Art. 2 erfasst unter anderem die Anbieter, die KI-Systeme in der EU in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck (sog. «GPAI»-Modelle[13]) in Verkehr bringen, unabhängig von deren Sitz (EU oder Drittland); Betreiber mit Sitz oder Aufenthalt in der EU; Anbieter und Betreiber in Drittstaaten, wenn KI-Ergebnisse in der EU verwendet, werden; Importeure und Händler sowie Produkthersteller, die KI-Systeme unter eigenen Namen oder eigener Marke zusammen mit einem Produkt in Verkehr bringen oder in Betrieb nehmen.

Der AI Act ist risikobasiert: KI-Systeme mit unannehmbaren Risiken sind mit Ausnahmen verboten, etwa Social Scoring (Art. 5)[14]. Hochrisiko-KI-Systeme sind zulässig, unterliegen aber strengen Anforderungen wie Risikobewertung, Datenqualität und Dokumentation (Art. 5–27)[15]. KI-Systeme mit begrenztem Risiko unterstehen spezifischen Transparenzpflichten (Art. 50). Systeme mit keinem oder minimalem Risiko lösen keine Pflichten aus. Für GPAI-Modelle gelten eigenständige, abgestufte Pflichten (Art. 51–55), etwa Cybersicherheit für Modelle und physische Infrastruktur sowie Governance- und Nachweispflichten bei systemischen Risiken.

Der Governance-Rahmen umfasst das AI Office der Europäischen Kommission (Art. 64) sowie nationale Marktüberwachungs- und notifizierende Behörden (Art. 70). Das AI Office beobachtet und überwacht KI-Systeme und GPAI-Modelle, entwickelt Praxisleitfäden, Vorlagen und Instrumente, unterstützt Behördenkoordination, berät bei der Einstufung von KI-Modellen, entwickelt Bewertungs- und Testmethoden und wirkt bei Identifizierung und Minderung systemischer Risiken mit. Das Sanktionssystem (Art. 99 ff.) sieht bei verbotenen KI-Praktiken Bussen bis 35 Millionen Euro oder 7 Prozent des weltweiten Jahresumsatzes, bei anderen zentralen Pflichtverletzungen bis 15 Millionen Euro oder 3 Prozent, bei falschen oder irreführenden Auskünften bis 7,5 Millionen Euro oder 1 Prozent vor; für KMU und Start-ups gelten reduzierte Höchstbeträge. Sanktionen müssen wirksam, verhältnismässig und abschreckend sein. Für die Schweiz ist der AI Act nicht bindend, wirkt aber extraterritorial, wenn Schweizer Anbieter oder Betreiber KI-Systeme oder GPAI-Modelle in der EU in Verkehr bringen, in Betrieb nehmen oder Ergebnisse in der EU verwendet werden[16].

3.3. KI-Regulierung in der Schweiz

Im Kanton Zug und in der Schweiz gibt es derzeit keine spezifischen gesetzlichen Grundlagen nur für KI-Anwendungen. KI entwickelt sich in einer bereits bestehenden Rechtsordnung, die auch für KI gilt.[17] Die Regulierung erfolgt durch bestehende nationale Gesetze und kantonale Bestimmungen. Solange die Vorgaben der geltenden, technologieneutralen Rechtsordnung eingehalten werden, steht dem Einsatz von KI-Anwendungen grundsätzlich nichts entgegen.

---

[13] Ein sog. GPAI-Modell («General Purpose AI» oder «KI-Modell mit allgemeinem Verwendungszweck») wird gemäss Art. 3 Ziff. 63 AI Act definiert als «KI-Modell – einschliesslich der Fälle, in denen ein solches KI-Modell mit einer grossen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden». Gemäss BJ sind solche GPAI-Modelle aufgrund der vielseitigen Einsetzbarkeit und der Bewältigung von zahlreichen Aufgaben (z. B. Textgenerierung, Bildverarbeitung oder Sprachübersetzung) mit höheren Risiken verbunden (BAKOM, Auslegeordnung, S. 10).

[14] KI-Systeme, die der Einstufung natürlicher Personen aufgrund ihres sozialen Verhaltens dienen.

[15] BAKOM, Auslegeordnung, S 9.

[16] Die Rechtliche Basisanalyse enthält in Kapitel 5, S. 89–132, detaillierte Ausführungen zum AI Act und dessen Auswirkungen auf die Schweizer Rechtsordnung.

[17] Bundesrat, Leitlinien «Künstliche Intelligenz» für den Bund, S. 9 (https://www.sbfi.admin.ch/dam/de/sd-web/-uy97trD1VMc/Leitlinien%2520K%C3%BCnstliche%2520Intelligenz%2520-%2520DE%5B1%5D.pdf; besucht am 5. März 2026).

3.3.1. Legalitätsprinzip

Das Legalitätsprinzip (Art. 5 Abs. 1 BV) verlangt, dass jede staatliche Tätigkeit nur aufgrund und nach Massgabe generell abstrakter Normen ausgeübt werden darf, die genügend bestimmt sind. Bezüglich des Erfordernisses der genügenden Bestimmtheit eines Rechtssatzes wird allerdings nicht verlangt, dass staatliches Handeln bis in alle Einzelheiten detailliert vorprogrammiert ist. Gemäss Rechtsprechung des Bundesgerichts wird immerhin gefordert, «dass der Bürger sein Verhalten danach richten und die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Gewissheit erkennen kann»[18]. In zahlreichen Bereichen wird das Handeln nur durch marginale rechtliche Vorgaben gesteuert. Dies ist etwa der Fall im Bereich der sogenannten Bedarfsverwaltung[19], wo es um die Beschaffung der zur Erfüllung der öffentlichen Aufgaben erforderlichen Sachmittel und Dienstleistungen geht (z. B. IKT-Mittel für die Textverarbeitung). In diesem Bereich genügt es, wenn für die Aufgabe eine genügende Rechtsgrundlage besteht. Mit der Begründung der Aufgabe wird auch die Kompetenz verliehen, die dafür erforderlichen Mittel zu beschaffen[20]. Inhaltlich wichtige Rechtsnormen sind in einem Gesetz im formellen Sinn zu erlassen. Bei schwerwiegenden Grundrechtseinschränkungen verlangt Art. 36 Abs. 1 BV eine Grundlage in einem solchen Gesetz. Eine Verordnung des Regierungsrats genügt nicht.

Für KI ist vor allem die Konkretisierung des Legalitätsprinzips in § 5 des Datenschutzgesetzes (DSG) vom 28. September 2000 (BGS 157.1) relevant. Für die Bearbeitung von besonders schützenswerten Personendaten[21] oder bei einem Profiling[22] braucht es eine genügend bestimmte Grundlage in einem Gesetz im formellen Sinn. Bei nicht besonders schützenswerten Personendaten genügt eine genügend bestimmte Grundlage in einer Verordnung.

3.3.2. Grundrechte

Unter Grundrechten versteht man unter anderem die in Art. 7 ff. BV, § 3 ff. der Verfassung des Kantons Zug (Kantonsverfassung, KV) vom 31. Januar 1894 (BGS 111.1) und die von internationalen Menschenrechtskonventionen (EMRK, Internationaler Pakt über bürgerliche und politische Rechte und andere internationale Abkommen) gewährleisteten grundsätzlichen Rechte des Einzelnen gegenüber dem Staat. Zu den Grundrechten gehören auch die allgemeinen Verfahrensgarantien gemäss Art. 29 BV bzw. § 5 und 7 KV und die Garantien für das gerichtliche Verfahren gemäss Art. 30 BV bzw. § 6 KV[23]. Die Grundrechte sind von den Behörden in sämtlichen Bereichen ihrer Tätigkeit zu beachten.

a) Verfahrensgarantien

Im KI-Kontext sind insbesondere die allgemeinen Verfahrensrechte (Verfahrensgarantien) gemäss Art. 29 BV beziehungsweise § 5 und § 7 KV von Bedeutung. Sie richten sich an alle Verfahrensbeteiligten und sind auch von den Behörden in sämtlichen Verfahren zu berücksichtigen. Dazu gehört unter anderem der Anspruch auf rechtliches Gehör. Dieses umfasst das Recht einer Partei, in einem Gerichts- oder Verwaltungsverfahren mit ihren Begehren angehört

---

18 BGE 138 IV 13 E. 4.1.

19 Benjamin Schindler, St. Galler Kommentar zu Art. 5 BV, Rz. 29 ff.

20 Tobias Jaag, in: Bedarfsverwaltung, Festschrift, Bern 2011, S. 554.

21 Als besonders schützenswerte Personendaten gelten gemäss § 2 Abs. 1 Bst. b DSG alle Angaben über die religiösen, weltanschaulichen, politischen und berufspolitischen Ansichten oder Tätigkeiten, die Intimsphäre, die Gesundheit, die ethnische Zugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative und strafrechtliche Verfolgungen und Sanktionen. Ebenso fallen darunter biometrische Daten, die mittels technischer Verfahren die eindeutige Identifizierung einer natürlichen Person erlauben, sowie genetische Daten.

22 Profiling ist nach § 2 Abs. 1 Bst. b1 DSG jede, insbesondere automatisierte, Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, namentlich bezüglich Arbeitsleistung, politischer Meinungsbildung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität.

23 Ulrich Häfelin, Walter Haller, Helen Keller, Daniela Thurnherr, Schweizerisches Bundesstaatsrecht, 11. Auflage, Zürich/Basel/Genf 2016, N. 200 (nachfolgend: Häfelin, Haller, Müller, Thurnherr, Schweizerisches Bundesstaatsrecht).

zu werden, Einsicht in die Akten zu nehmen und zu den für den Entscheid wesentlichen Punkten Stellung nehmen zu können, bevor dieser gefällt wird.

Eine Einschränkung durch KI ist grundsätzlich nur bei vollautomatisierten Einzelentscheidungen denkbar, bei denen sich die Partei nur zu Beginn äussern kann und der weitere Ablauf ohne menschliche Intervention erfolgt. Vollautomatische Entscheide kommen daher nur in Betracht, wenn den Begehren der betroffenen Person entsprochen wird[24]. Eine vergleichbare Regelung enthält auch Art. 21 des Bundesgesetzes über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020 (SR 235.1)[25]. Besteht ein Ermessens- oder Beurteilungsspielraum der Behörde, ist auf vollautomatisierte Entscheide zu verzichten[26].

In Gegenwart und absehbarer Zukunft steht der unterstützende Einsatz von KI für Recherchen, Entwürfe und Informationsverarbeitung im Vordergrund. Dabei verbleibt die Entscheidverantwortung bei der zuständigen Behörde beziehungsweise den entscheidenden Personen: Eine spezifische Rechtsgrundlage ist dafür grundsätzlich nicht erforderlich, sofern Datenschutz-, Geheimhaltungs- und Verfahrensrecht eingehalten werden.

b) Verfahrensgrundsätze

Das Untersuchungsprinzip verpflichtet Verwaltung und Justiz, den Sachverhalt von Amtes wegen abklären[27]. Das bedeutet, dass die Behörden für die Ermittlung der Entscheidgrundlagen zuständig sind und alle rechtserheblichen Informationen erheben müssen (siehe z. B. § 12 des Gesetzes über den Rechtsschutz in Verwaltungssachen [Verwaltungsrechtspflegegesetz, VRG] vom 1. April 1976 [BGS 162.1]). Die genutzten Daten müssen vollständig, korrekt und verfügbar sein; fachgesetzlich müssen notwendige Zugriffsrechte auf Datensammlungen oder Mitwirkungspflichten der Parteien bestehen. Bei vollautomatisierten Einzelentscheiden trifft die Behörde keine eigenen Abklärungen, was die Gefahr standardisierter Datenerhebung oder der Vernachlässigung einzelfallspezifischer Informationen erhöht [28]. Bei teilautomatisierten Entscheiden lassen sich rechtliches Gehör, Rechtsgleichheit und Diskriminierungsverbot leichter wahren, weil eine natürliche Person die inhaltliche Bewertung vornimmt und Stellungnahmen ermöglichen kann [29].

c) Diskriminierungsverbot

Die Sicherstellung der Vollständigkeit und Korrektheit der genutzten Daten ist auch erforderlich, um den Anspruch auf rechtsgleiche Behandlung und das Diskriminierungsverbot gemäss Art. 8 BV bzw. § 5 KV sicherstellen zu können. Beim Einsatz von KI in Verfahren vor Behörden besteht jedoch nach allgemeiner Lehrauffassung ein erhebliches Diskriminierungspotenzial[30]. KI in Behördenverfahren birgt erhebliches Diskriminierungspotenzial, etwa durch präexistierenden Bias in Trainingsdaten, Stereotypen, Zielsetzungen des Bestellers oder Systemdesigners, technische Limitierungen der Systemarchitektur oder im Betrieb entstehende diskriminierende Muster. Behörden müssen Verfahren so ausgestalten, dass Diskriminierungen ausgeschlossen werden: Trainings- und Sachverhaltsdaten müssen vollständig, korrekt und rechtserheblich geeignet sein. Prüf-, Dokumentations- und Transparenzmechanismen sind vorzusehen, damit Entscheidgrundlagen nachvollziehbar bleiben und Diskriminierungen früh erkannt und beseitigt

---

[24] David Rechsteiner, Der Algorithmus verfügt, Verfassungs- und verwaltungsrechtliche Aspekte automatisierter Einzelentscheidungen, in: Jusletter vom 26. November 2018, Rz. 23. Siehe auch Nadja Braun Binder, Nina Laukenmann, Liliane Obrecht, KI in der Verwaltung: Entwicklungen und Herausforderungen, in: Jusletter IT vom 4. Juli 2024, Rz. 22 (nachfolgend: Braun Binder, Laukenmann, Obrecht, KI in der Verwaltung).

[25] Im Folgenden wird die Abkürzung «DSG» jeweils nur für das kantonale Datenschutzgesetz verwendet.

[26] ZH-Schlussbericht, S. 47.

[27] Ulrich Häfelin, Georg Müller, Felix Uhlmann, Allgemeines Verwaltungsrecht, 8. Auflage, Zürich 2020, N. 988 (nachfolgend: Häfelin, Müller, Uhlmann, Allgemeines Verwaltungsrecht).

[28] Braun Binder, Laukenmann, Obrecht, KI in der Verwaltung, Rz. 25.

[29] ZH-Schlussbericht, S. 37.

[30] ZH-Schlussbericht, S. 39 ff.

werden. Für voll- und teilautomatisierte Bearbeitungen sind menschliche Kontroll- und Eingriffsmöglichkeiten vorzusehen, um verfassungsrechtliche Vorgaben, insbesondere Art. 8 Abs. 2 BV, einzuhalten und fehlerhafte oder unangemessene Entscheide im Einzelfall korrigieren zu können [31].

3.3.3. Datenschutz

Das Datenschutzrecht konkretisiert das Grundrecht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV), schützt die Privatsphäre natürlicher Personen und regelt datenbearbeitender Stellen sowie die Rechte der betroffenen Personen. Das kantonale Datenschutzgesetz (DSG) lässt Personendatenbearbeitungen zu, wenn das Legalitätsprinzip und die im DSG verankerten Bearbeitungsgrundsätze eingehalten werden. Nach § 5 DSG dürfen Organe der Verwaltung und Justiz Personendaten elektronisch bearbeiten, wenn sie

- entweder über eine explizite, unmittelbare gesetzliche Grundlage verfügen (Verordnung bei Personendaten [§ 5 Abs. 1 Bst. a DSG], Gesetz im formellen Sinn bei besonders schützenswerten Personendaten oder einem Profiling [§ 5 Abs. 2 Bst. a DSG]) das heisst über eine Grundlage, die genau regelt, wer welche Daten, zu welchem Zweck, bearbeiten darf, oder
- wenn die Datenbearbeitung für eine in einer gesetzlichen Grundlage umschriebenen Aufgabe unentbehrlich ist (§ 5 Abs. 1 Bst. b DSG) beziehungsweise wenn die Datenbearbeitung bei besonders schützenswerten Personendaten oder einem Profiling für eine in einem formellen Gesetz umschriebene Aufgabe offensichtlich unentbehrlich ist (§ 5 Abs. 2 Bst. b DSG), das heisst, wenn eine sogenannte bloss mittelbare gesetzliche Grundlage vorliegt, welche die zu erfüllende Aufgabe nur umschreibt. «Offensichtlich unentbehrlich bedeutet, dass die in einem formellen Gesetz umschriebene Aufgabe ohne Bearbeitung der entsprechenden Daten gar nicht erledigt werden könnte[32].

Als Bearbeitung gilt dabei nach § 2 Abs. 1 Bst. c DSG «jeder Umgang mit Personendaten, *unabhängig von den angewandten Mitteln und Verfahren*, insbesondere das Erheben, Beschaffen, Aufzeichnen, Sammeln, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Austauschen, Zusammenführen, Archivieren, Löschen oder Vernichten sowie Durchführen logischer beziehungsweise rechnerischer Operationen mit Personendaten».

Die Bearbeitungsgrundsätze verlangen insbesondere, dass Personendaten nur unter Beachtung des Prinzips der Verhältnismässigkeit und des Grundsatzes von Treu und Glauben bearbeitet werden dürfen (§ 4 Abs. 1 Bst. d DSG). Zu beachten ist auch der Grundsatz der Zweckbindung, wonach Personendaten nur für Zwecke bearbeitet werden dürfen, die bei der Beschaffung angegeben worden sind, aus den Umständen ersichtlich oder gesetzlich vorgesehen sind (Transparenzprinzip; § 4 Abs. 1 Bst. c DSG). Ferner müssen die Personendaten, die bearbeitet werden sollen, aktuell, richtig und vollständig sein (§ 4 Abs. 1 Bst. a DSG) und die Sicherheit aller Personendaten muss durch angemessene technische und organisatorische Massnahmen sichergestellt werden (Informationssicherheit; § 7 Abs. 1 DSG). Die Organe sind verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden (sog. «Privacy by Design»; § 7a Abs. 1 DSG). Zudem müssen die Organe die betroffene Person über die Beschaffung von Personendaten informieren (§ 6a und § 6b DSG) und Personendaten, die es nicht mehr benötigt, anonymisieren oder vernichten, soweit die Daten nicht unmittelbaren Beweiszwecken dienen oder dem zuständigen Archiv abzuliefern sind (§ 11 DSG).

---

[31] ZH-Schlussbericht, S. 40, 57 und 63.

[32] Bericht und Antrag des Regierungsrats vom 7. Dezember 1999 (Vorlage Nr. 733.1 - 10042) zum Erlass eines Datenschutzgesetzes, S. 19.

Seit der Teilrevision vom 1. September 2020 braucht es bei neuer oder wesentlich geänderter elektronischer Bearbeitung von Daten einer grösseren Anzahl betroffener Personen zusätzlich zur Rechtsgrundlage eine Datenschutz-Folgenabschätzung (DSFA) nach § 7b DSG und § 5a VIP. In der Initialisierungsphase sind Rechtsgrundlagenanalyse und Schutzbedarfsanalyse zu erstellen. Erstere klärt die genügende Rechtsgrundlage nach § 5 DSG, Letztere, ob eine DSFA-Risikoanalyse und allenfalls ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) nötig sind. In der Konzeptphase sind bei Bedarf DSFA-Risikoanalyse und ISDS-Konzept zu erstellen; sie bestimmen Risiken für Grundrechte, Massnahmen zu deren Eliminierung oder Minimierung sowie Details von Bearbeitung, Fachanwendung, IT-Umgebung und technischen sowie organisatorischen Massnahmen. Ergibt die DSFA ein hohes Restrisiko oder steht der Vorgang auf der Liste Vorabkonsultation der Datenschutzstelle, ist nach § 19a DSG eine Vorabkonsultation durchzuführen. Auf der Liste stehen etwa automatisierte Entscheidfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung, Cloud-Datenbearbeitungen, Bearbeitung von Daten schutzbedürftiger Personen und biometrischen Daten. Soweit KI Personendaten bearbeitet, ist Datenschutzrecht deshalb ein zentrales Rechtsgebiet, gerade wegen erhöhter Grundrechtsrisiken.[33], müssen die geplante Datenbearbeitung inklusive alle für die DSFA erstellten Dokumente der Datenschutzstelle zur sogenannten Vorabkonsultation gemäss § 19a DSG eingereicht werden. Auf der «Liste Vorabkonsultation» sind zum Beispiel die automatisierte Entscheidfindung mit Rechtswirkung oder ähnlicher bedeutsamer Wirkung für eine betroffene Person, die Datenbearbeitungen in der Cloud, die Bearbeitung von Daten schutzbedürftiger Personen oder die Bearbeitung von biometrischen Daten aufgeführt. Nach erfolgtem Abschluss der Vorabkonsultation kann die geplante Datenbearbeitung realisiert werden.

3.3.4. Schutz des geistigen Eigentums

Bei der Bearbeitung und Nutzung von Daten, die durch das Urheberrecht geschützt sind, sind das Bundesgesetz über die Erfindungspatente (Patentgesetz, PatG; SR 232.14), das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG; SR 231.1) zu beachten.

a) Patentrecht

Im Patentrecht stellen sich Fragen der Patentierbarkeit von KI, der Erfinderschaft und der Offenlegung. Patentierbar sind nach Art. 1 PatG nur technische Lösungen für technische Probleme, die neu, erfinderisch und gewerblich anwendbar sind. Abstrakte Ideen, mathematische Methoden, Algorithmen oder Lernverfahren sind ausgeschlossen; Computerprogramme als solche ebenfalls, können aber Teil einer patentfähigen technischen Erfindung sein, etwa bei einem KI-gestützten Bildgebungsverfahren in der Medizintechnik. Als Erfinderin oder Erfinder ist nach geltendem Recht zwingend eine natürliche Person zu nennen, auch wenn der Erfindungsprozess teilweise oder vollständig automatisiert erfolgte; das Bundesverwaltungsgericht bestätigte dies im Entscheid B-2532/2024 («DABUS»). Unklar ist, in welchem Umfang Trainingsdaten, Modellarchitekturen oder Algorithmen in Patentanmeldungen offenzulegen sind, obwohl sie für Nachvollziehbarkeit, Patentfähigkeit und Reproduzierbarkeit wesentlich sein können. Generative KI kann zudem das Volumen wissenschaftlicher und technischer Fachliteratur erhöhen; diese gehört zum Stand der Technik und kann Neuheit sowie erfinderische Tätigkeit erschweren.

b) Urheberrecht

Im Urheberrecht setzt Schutz eine menschliche geistige Schöpfung mit individuellem Charakter voraus (Art. 2 Abs. 1 und Art. 6 Abs. 1 URG). Vollständig maschinell erzeugte Inhalte geniessen in der Regel keinen urheberrechtlichen Schutz. Bei Kombination von maschineller

---

[33] https://zg.ch/dam/jcr:04dd6734-2225-4efd-a463-92efe413eac4/Liste%20Vorabkonsultation.pdf (besucht am 5. März 2026); ZH-Schlussbericht, S. 46.

Generierung und menschlicher Mitwirkung ist zu prüfen, ob der menschliche Beitrag als eigene geistige Schöpfung erkennbar ist; nach bundesgerichtlicher Rechtsprechung genügt ein geringer Grad selbständiger geistiger Tätigkeit, sofern der individuelle Charakter im Werk sichtbar wird. Das Training von KI-Systemen verwendet regelmässig grosse Datenmengen mit geschützten Werken und kann Vervielfältigungen nach Art. 10 Abs. 2 URG auslösen, insbesondere bei dauerhafter Speicherung oder Übernahme in Modellparameter. Zu prüfen ist jeweils, ob Schrankenbestimmungen wie betriebsinterner Gebrauch (Art. 19 Abs. 1 Bst. c URG), vorübergehende Vervielfältigung (Art. 24a URG) oder Werkverwendung zu wissenschaftlichen Zwecken (Art. 24d URG) anwendbar sind; jede Schranke ist einzelfallbezogen und voraussetzungsgebunden.

Beim Einsatz von KI im Bereich des Urheberrechts stellt sich zunächst die grundlegende Frage nach der Schutzfähigkeit von KI-Erzeugnissen. Nach geltendem URG setzt der urheberrechtliche Schutz eines Werkes voraus, dass es sich um eine geistige Schöpfung mit individuellem Charakter handelt, die von einem Menschen geschaffen wurde (Art. 6 Abs. 1 URG). Diese Anforderung ergibt sich unmittelbar aus Art. 2 Abs. 1 URG, wonach Werke «geistige Schöpfungen der Literatur und Kunst» sind, die einen «individuellen Charakter» haben. KI-Systeme können jedoch keine Urheber im Rechtssinn sein, weshalb Inhalte, die vollständig maschinell erzeugt werden, in der Regel keinen urheberrechtlichen Schutz geniessen.

3.3.5. Geheimhaltungspflichten

a) Amtsgeheimnis

Der Einsatz von KI in der öffentlichen Verwaltung das Amtsgeheimnis, wie es insbesondere in Art. 320 des Schweizerischen Strafgesetzbuches (StGB) vom 21. Dezember 1937 (SR 311.0) geregelt ist. Strafbar ist, wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist oder das er in seiner amtlichen oder dienstlichen Stellung oder als Hilfsperson eines Beamten oder einer Behörde wahrnahm (Abs. 1). Die Weitergabe von Informationen an ein KI-System kann eine Offenbarung sein, wenn sie an eine nicht autorisierte Stelle erfolgt. Im Kanton Zug ist insbesondere § 29 des Gesetzes über das Arbeitsverhältnis des Staatspersonals (Personalgesetz, PG) vom 1. September 1994 (BGS 154.21) zentral. Mitarbeiterinnen und Mitarbeitern dürfen unter Vorbehalt von § 28bis und § 28ter PG sowie § 51 Abs. 2 des Gesetzes über den Finanzhaushalt des Kantons und der Gemeinden (Finanzhaushaltgesetz, FHG) vom 31. August 2006 (BSG 611.1) Drittpersonen und anderen Amtsstellen keine Tatsachen mitteilen, an denen ein öffentliches Geheimhaltungsinteresse, ein Persönlichkeitsschutzinteresse oder eine besondere Geheimhaltungspflicht besteht.

Auslagerungen an externe KI- oder Cloud-Dienstleister sind nicht von vornherein unzulässig, verlangen aber, dass Amtsgeheimnis, Datenschutz und Informationssicherheit verbindlich gewahrt bleiben[34]. Diese dürfen die Daten jeweils nur so bearbeiten, wie der Auftraggeber, also die Behörde, dies auch selbst tun dürfte (§ 6 Abs. 1 Bst. a DSG). Zudem muss die Behörde sicherstellen, dass auch der beauftragte Dritte die Grundsätze des Datenschutzes und die Informationssicherheit gewährleistet sowie die Rechte der betroffenen Personen wahrt (§ 6 Abs. 2 DSG). In der Praxis wird dies durch entsprechende Vertragsbestimmungen, Sicherheitsauflagen und technische Zugriffsbeschränkungen umgesetzt. Hiervon ausgenommen sind Auslagerungen, wenn gesetzliche oder vertragliche Verpflichtungen eine solche verbieten (§ 6 Abs. 1 Bst. b DSG)[35]. Seit der Revision von Art. 320 StGB (in Kraft seit 1. Januar 2023) werden auch externe Informatikleistungserbringer einer Behörde inklusive für sie handelnde Personen als

[34] Bei den Dritten handelt es sich in aller Regel um sog. Auftragsdatenbearbeiter nach § 6 Abs. 1 DSG.
[35] Roger Plattner, Digitales Verwaltungshandeln – Rechtliche Aspekte der Digitalisierung in der öffentlichen Verwaltung, Zürich 2021, S. 52 (nachfolgend: Roger Plattner, Digitales Verwaltungshandeln).

Hilfsperson einer Behörde qualifiziert, was zur Folge hat, dass auch sie dem Amtsgeheimnis und der Strafbarkeit von Art. 320 StGB unterstehen.

b) Berufsgeheimnis

Das Berufsgeheimnis gemäss Art. 321 und Art. 321bis StGB verpflichtet Angehörige bestimmter Berufsgruppen, namentlich Ärzte, Anwälte, Geistliche und weitere in der Norm aufgeführte Personen, zur Wahrung der ihnen in Ausübung ihres Berufs anvertrauten oder bekannt gewordenen Geheimnisse. Dazu gehört auch die Tatsache, dass zwischen einem Angehörigen einer dieser Berufsgruppen und einer Person ein spezifisches Verhältnis (z. B. Mandatsverhältnisse bei Anwälten oder Behandlungsverhältnisse zwischen Ärzten und Patienten) besteht. Zudem gilt das Berufsgeheimnis auch gegenüber Mitarbeitenden, soweit diese nicht in ein Mandat oder in ein Behandlungsverhältnis eingebunden sind. Im Kontext des Einsatzes von KI-Systemen in der öffentlichen Verwaltung sind hier die gleichen Vorgaben zu beachten wie beim Amtsgeheimnis.

c) Fabrikations- und Geschäftsgeheimnis

Das Fabrikations- und Geschäftsgeheimnis (Art. 162 StGB) schützt Betriebs- und Geschäftsgeheimnisse vor unbefugter Offenbarung durch Personen, die aufgrund ihrer Stellung oder Tätigkeit davon Kenntnis erlangt haben. Strafbar ist eine Offenbarung ohne Berechtigung, wenn sie geeignet ist, den Berechtigten zu schädigen. Der Schutzbereich umfasst sämtliche nicht allgemein bekannte technische, kommerzielle oder organisatorische Informationen, deren Geheimhaltung im berechtigten wirtschaftlichen Interesse liegt.

Beim Einsatz von KI entstehen besondere Risiken für die Integrität von Fabrikations- und Geschäftsgeheimnissen. KI-Systeme können im Rahmen von Datenverarbeitung, Speicherung oder Übermittlung geschützte technische Verfahren, Produktionsprozesse oder interne Geschäftsstrategien verarbeiten und dadurch potenziell Dritten zugänglich machen. Diese Gefahr besteht insbesondere bei der Nutzung externer Cloud-Infrastrukturen oder fremder Datenverarbeitungsdienste, wenn dort nicht sichergestellt ist, dass die Geheimhaltungspflichten uneingeschränkt fortbestehen. Für den rechtskonformen Einsatz ist deshalb entscheidend, dass vertrauliche Geschäfts- und Fabrikationsinformationen bei jeder Form der Datenbearbeitung vertraglich geschützt werden und die Weitergabe an Dritte ohne Zustimmung des Berechtigten ausgeschlossen bleibt. Dies gilt auch für KI-Trainingsprozesse, bei denen geschützte Inhalte in die Modellparameter einfliessen könnten.

Auch auf europäischer Ebene wird der Schutz von Geschäftsgeheimnissen ausdrücklich adressiert. Der AI Act nennt explizit den Schutz «vertraulicher Geschäftsinformationen oder Geschäftsgeheimnisse natürlicher oder juristischer Personen» und bezieht diesen Schutz auch auf Quellcodes. Für Schweizer Projekte mit EU-Bezug ist daher sicherzustellen, dass die Anforderungen beider Rechtsordnungen eingehalten werden.

3.3.6. Haftung

a) Haftpflichtrecht

In der Schweiz bestehen keine spezifischen haftpflichtrechtlichen Regelungen, die ausschliesslich für KI gelten. Massgeblich sind daher die allgemeinen Bestimmungen, insbesondere Art. 41 OR als haftpflichtrechtliche Generalklausel. Dieser sieht vor, dass für eine Haftung vier Voraussetzungen erfüllt sein müssen: Es muss ein Schaden vorliegen, dieser muss widerrechtlich verursacht worden sein, es muss ein adäquater Kausalzusammenhang bestehen und ein Verschulden nachgewiesen werden. Diese Grundsätze gelten auch für Schadensereignisse im Zusammenhang mit KI. Die Beweislast liegt grundsätzlich bei der geschädigten Partei. Bei hochkomplexen und intransparenten Systemen kann dies jedoch zu erheblichen Schwierigkeiten bei

der Durchsetzung von Ansprüchen führen, da der Ablauf, der zum Schaden geführt hat, oft nur schwer oder gar nicht nachvollzogen werden kann, namentlich wenn der Schaden durch das KI-System verursacht oder zumindest mitverursacht wurde.

In der EU wurde mit Blick auf diese Beweisprobleme der Einsatz zusätzlicher Instrumente wie erweiterter Offenlegungspflichten und widerlegbarer Kausalitätsvermutungen in einer eigenständigen KI-Haftungsrichtlinie vorgeschlagen.[36] Die KI-Haftungsrichtlinie wurde allerdings im Februar 2025 von der Europäischen Kommission offiziell zurückgezogen, weil sich im Gesetzgebungsprozess kein ausreichender politischer Konsens zwischen Rat und Parlament abzeichnete[37].

Solche spezifischen Bestimmungen existieren im schweizerischen Recht derzeit nicht. Zwar kennt die Schweizer Rechtsordnung gewisse prozessuale Möglichkeiten, um bei technisch bedingten Nachweisschwierigkeiten Beweiserleichterungen zu gewähren[38], jedoch fehlen im Kontext von KI ausdrückliche gesetzliche Vermutungen, wie sie in den EU-Vorschlägen enthalten waren. Für bestimmte Anwendungsbereiche bestehen jedoch bereits heute gewisse Beweiserleichterungen. So genügt beispielsweise für das Beweismass eine überwiegende Wahrscheinlichkeit, wenn ein strikter Beweis der Natur der Sache nach nicht möglich oder nicht zumutbar ist und entsprechend eine Beweisnot besteht. Hierzu gehört auch der Nachweis des Kausalzusammenhangs[39]. Zudem bestehen in zahlreichen Bereichen, in welchen KI-Systeme bereits heute zur Anwendung gelangen, verschuldensunabhängige Gefährdungshaftungen sowie ergänzende Versicherungspflichten, welche potenzielle Haftungslücken verhindern. Als Beispiele können hier die Halterhaftung für Motorfahrzeuge nach Art. 58 des Strassenverkehrsgesetzes (SVG) vom 19. Dezember 1958 (SR 741.01), die Haftung des Inhabers eines Eisenbahnunternehmens nach Art. 40b des Eisenbahngesetzes (EBG) vom 20. Dezember 1957 (SR 742.101), die Haftung für Luftfahrzeuge nach Art. 64 des Bundesgesetzes über die Luftfahrt (Luftfahrtgesetz, LFG) vom 21. Dezember 1948 (SR 748.0) oder letztlich auch die Werkeigentümerhaftung nach Art. 58 des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht; OR) vom 30. März 1911 (SR 220) genannt werden. Solche Gefährdungshaftungen bieten Betroffenen einen stärkeren Schutz als die allgemeine Verschuldenshaftung, da sie keine Verschuldensnachweise erfordern[40].

Im Vertragsrecht gilt bei Vertragsverletzungen eine Beweislastumkehr: Die Partei, die in Anspruch genommen wird, muss darlegen und beweisen, dass sie kein Verschulden trifft (Art. 97 Abs. 1 OR). In der Lehre wird bereits diskutiert, ob sich Verantwortliche bei Fehlfunktionen von KI-Systemen möglicherweise zu leicht entlasten könnten, indem sie auf die fehlende eigene Pflichtverletzung verweisen. Zur Diskussion steht eine Angleichung zu den Regeln der Hilfspersonenhaftung nach Art. 101 Abs. 1 OR: Danach sollen Fehler eines KI-Systems derjenigen Partei zugeordnet werden, welche das System einsetzt[41].

Bei Persönlichkeitsverletzungen, die durch den Einsatz von KI entstehen (z. B. Deepfakes), stehen Betroffenen die allgemeinen zivilrechtlichen Mittel des Persönlichkeitsschutzes zur Verfügung. Danach kann eine in ihrer Persönlichkeit verletzte Person zu ihrem Schutz gegen jede

---

36 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über ausservertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung) vom 28. September 2022 (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0496; besucht am 5. März 2026).

37 European Commission, Annexes to the Commission work programme 2025, Annex IV.

38 So sieht z. B. Art. 160 Abs. 1 Bst. b der Schweizerischen Zivilprozessordnung (Zivilprozessordnung, ZPO) vom 19. Dezember 2008 (SR 272) für die Parteien im Zivilverfahren eine Mitwirkungspflicht im Zusammenhang mit der Herausgabe von Urkunden (Editionspflicht) vor.

39 BJ, Rechtliche Basisanalyse, S. 144 f.

40 BJ, Rechtliche Basisanalyse, S. 144 ff.

41 BJ, Rechtliche Basisanalyse, S. 151.

andere Person ein Zivilgericht anrufen und verlangen, dass eine Persönlichkeitsverletzung beseitigt oder eine drohende Persönlichkeitsverletzung verboten wird (Art. 28a Abs. 1 Ziff. 1 und 2 ZGB). Die Bestimmungen zum Persönlichkeitsschutz im ZGB gelten als technikneutral und finden unabhängig davon Anwendung, ob die Verletzung durch ein menschliches Handeln oder durch eine KI verursacht wurde[42].

b) Produktehaftpflichtrecht

Die Produktehaftpflicht richtet sich nach dem Bundesgesetz über die Produktehaftpflicht (Produktehaftpflichtgesetz, PrHG) vom 18. Juni 1993 (SR 221.112.944). Es erfasst fehlerhafte Produkte mit verschuldensunabhängiger Herstellerhaftung und deckt Personenschäden sowie im privaten Gebrauch Sachfolgeschäden, nicht aber den Schaden am Produkt selbst (Art. 1 PrHG). Herstellerinnen sind Produzentinnen von End-, Grund- oder Teilprodukten, Quasi-Herstellerinnen und Importeurinnen (Art. 2 PrHG). Produkt ist jede bewegliche Sache und Elektrizität (Art. 3 PrHG); fehlerhaft ist ein Produkt, wenn es nicht die berechtigterweise erwartete Sicherheit bietet, insbesondere mit Blick auf Präsentation, vernünftigerweise erwartbaren Gebrauch und Zeitpunkt des Inverkehrbringens (Art. 4 Abs. 1 PrHG).

In der Schweiz ist schon seit längerem umstritten, ob «reine» Software im Sinne des PrHG unter den Produktebegriff fällt. Bisher musste sich das Bundesgericht dazu nicht äussern. Unbestritten ist bisher, dass Software im Zusammenhang mit einem körperlichen Produkt unter das PrHG fällt[43]. Herausfordernd ist zudem, den Begriff des Produktfehlers auf KI-Systeme anzuwenden. Während sich ein Konstruktions- oder Fabrikationsfehler bei physischen Produkten meist eindeutig feststellen lässt, sind Fehler bei KI-Systemen oft das Ergebnis komplexer, dynamischer Prozesse. Fehlerhafte Ergebnisse können auf unvollständigen oder verzerrten Trainingsdaten beruhen, auf unerwarteten Interaktionen des Systems mit seiner Umgebung oder auf automatischen Aktualisierungen («Weiterlernen»), die erst nach der Auslieferung erfolgen. Solche Eigenschaften erschweren den Nachweis, dass ein Fehler bereits im Zeitpunkt des Inverkehrbringens vorlag, wie es das PrHG voraussetzt.

Ein weiterer Problempunkt ist die Frage des Schadensnachweises und der Kausalität. In klassischen Produkthaftungsfällen lässt sich meist ein direkter Zusammenhang zwischen einem Defekt und einem Schaden belegen. Bei KI-Systemen hingegen können sich fehlerhafte Entscheidungen in komplexen Kausalketten niederschlagen, bei denen der ursächliche Beitrag des Systems schwer isolierbar ist. Dies gilt insbesondere für Anwendungen, die nicht autonom, sondern im Zusammenspiel mit menschlichen Entscheidungen agieren. Hier stellt sich die Frage, ob bestehende Beweisregeln und Beweiserleichterungen – wie etwa die Beweislastumkehr in gewissen Konstellationen – auf KI-gestützte Produkte anwendbar sind oder ob gesetzliche Anpassungen erforderlich werden.

Schliesslich stellt sich die Frage nach der Verantwortlichkeit in mehrgliedrigen Wertschöpfungsketten. KI-Systeme entstehen häufig durch die Kombination von Komponenten verschiedener Hersteller – etwa einer Hardwareplattform, einer Standardsoftware, spezifischer KI-Module und durch den Betreiber erstellter Trainingsdaten. Diese Fragmentierung der Herstellung und Wartung erschwert die Zuordnung der Haftung zu einer einzelnen verantwortlichen Partei. Je nach Konstellation könnte es erforderlich sein, Haftungstatbestände klarer zu definieren, um sowohl den Schutz der Geschädigten zu gewährleisten als auch die Rechtssicherheit für Hersteller und Betreiber zu erhöhen.

---

[42] BJ, Rechtliche Basisanalyse, S. 149.

[43] BJ, Rechtliche Basisanalyse, S. 148; Vito Roberto, Produkthaftpflicht und Software, in: Jahrbuch des Schweizerischen Konsumentenrechts (JKR) 2000, Bern 2000, S. 59.

In der EU wurde 2024 die alte Richtlinie über die Haftung für fehlerhafte Produkte von 1985[44] durch eine neue Produkthaftungsrichtlinie[45] ersetzt, um der zunehmenden Digitalisierung von Produkten Rechnung zu tragen. Die neue Richtlinie enthält eine verschuldensunabhängige Herstellerhaftung auch für Hersteller von Software einschliesslich KI-Systemen. Mit der Revision wollte der europäische Gesetzgeber unter anderem erreichen, dass die Hersteller vor dem Hintergrund der Entwicklungen in der Informatik die Kontrolle und auch die Einflussnahme ihrer Produkte beim Inverkehrbringen behalten. Erweitert wurden auch der Kreis der Haftenden: Neu fallen auch Entwickler oder Hersteller von Software einschliesslich die Anbieter von KI-Systemen unter den Herstellerbegriff. Auch der Fehlerbegriff wurde erweitert auf fehlerhafte Updates und bei Software und auf Schwachstellen in der Cybersicherheit. Zudem wurde die Deckung von Schäden bei Personen oder Sachen auf Daten ausgedehnt, das heisst ein Verlust oder eine Verfälschung von Daten durch fehlerhafte KI-Systeme können inskünftig ebenfalls eine Schadenersatzpflicht auslösen[46].

Analog zu der von der EU-Kommission vorgesehenen Richtlinie über die KI-Haftung wird möglichen Beweisschwierigkeiten für Parteien in einem zivilrechtlichen Verfahren mit Offenlegungspflichten (Art. 9 EU-Produkthaftungsrichtlinie: Offenlegung von Beweismitteln) und Kausalitätsvermutungen (Art. 10 EU-Produkthaftungsrichtlinie: Beweislast) entgegengetreten[47].

3.3.7. KI im öffentlich-rechtlichen Arbeitsverhältnis

KI-Systeme sind in der modernen Arbeitswelt bereits stark verbreitet. Einerseits hat der Einsatz von sogenannten «Automated Decision-Making Systems» (ADM-Systeme) in unterschiedlichen Bereichen der Arbeitswelt zugenommen. So werden automatisierte Entscheidsysteme in den Bereichen «Hiring & Recruting», «Performance Management» oder «Compliance Management» vermehrt eingesetzt[48]. Andererseits werden KI-Systeme von den Arbeitnehmenden zunehmend als Arbeitsmittel genutzt, was neue rechtliche Fragestellungen insbesondere im Hinblick auf Datenschutz, Informationssicherheit oder Amtsgeheimnis aufwirft.

Schweizerische Unternehmensbefragungen von 2018 und 2020 haben im Bereich des KI-Einsatzes einen deutlichen Anstieg verzeichnet. Verbreitet sind etwa automatisierte Vorprüfungen von Bewerbungen sowie Instrumente zur IT-Nutzungs- und Internetüberwachung[49]. Daraus ergeben sich zentrale Herausforderungen[50]:

- Beim Datenschutz können umfangreiche, kontinuierliche und teils undifferenzierte Bearbeitungen von Personendaten mit unklaren Zwecken auftreten.
- Im Gesundheitsschutz können Leistungs- und Überwachungstools das psychische Wohlbefinden beeinträchtigen oder Überlastungssituationen erzeugen, wenn unrealistische Leistungsparameter zugrunde liegen.
- Im Rahmen der Leistungsbewertung kann der Einsatz von KI persönliche Qualitäten oder soziale Kompetenzen sowie Besonderheiten einer konkreten Situation unzureichend abbilden und dadurch zu starren, teilweise unrealistischen Leistungsurteilen führen.
- Ein zentrales Risiko ist auch die diskriminierende Verzerrung, insbesondere in Rekrutierungsprozessen.

---

44 Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:31985L0374; besucht am 5. März 2026).

45 Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402853; besucht am 5. März 2026).

46 BJ, Rechtliche Basisanalyse, S. 146 f.

47 BJ, Rechtliche Basisanalyse, S. 147.

48 Isabelle Wildhaber / Isabel Ebert, Beteiligung der Arbeitnehmenden beim Einsatz von ADM-Systemen am Arbeitsplatz, Studie der Universität St. Gallen im Auftrag von AlgorithmWatch CH und syndicom Gewerkschaft Medien und Kommunikation, St. Gallen 2023, S. 5 (https://www.alexandria.unisg.ch/server/api/core/bitstreams/ce7de92a-cbe5-4651-820a-ff9d3347c4fa/content; besucht am 5. März 2026).

49 BJ, Rechtliche Basisanalyse, S. 157.

50 BJ, Rechtliche Basisanalyse, S. 157.

- Transparenz und Begründbarkeit von Entscheidungen sind von besonderer Bedeutung, da häufig unklar bleibt, auf welcher Grundlage algorithmische Resultate beruhen.

Für das öffentlich-rechtliche Arbeitsverhältnis im Kanton Zug gelten insbesondere das Gesetz über das Personalgesetz (PG), die Vollziehungsverordnung zum Gesetz über das Arbeitsverhältnis des Staatspersonals (Personalverordnung, PVO) vom 12. Dezember 1994 (BGS 154.21) und das kantonale Datenschutzrecht. KI kann Personalrekrutierung, Leistungsbeurteilung, Weisungen oder personalrechtliche Massnahmen betreffen und berührt regelmässig auch Fragen der Bearbeitung von Personendaten. Darüber hinaus sind beim Einsatz von KI im öffentlich-rechtlichen Arbeitsverhältnis weitere Rechtsgrundlagen zu beachten. Als staatlicher Arbeitgeber ist der Kanton an die verfassungsmässigen Grundrechte gebunden.

Neben den Pflichten des Arbeitgebers bestehen auch Pflichten der Mitarbeitenden. Der Kanton Zug hat hierzu ein Merkblatt zur Nutzung von generativer KI erlassen. Danach ist bei der Nutzung von KI-Systemen insbesondere sicherzustellen, dass keine vertraulichen oder personenbezogenen Daten unzulässig in externe Systeme eingegeben werden, dass rechtliche Vorgaben – namentlich Datenschutz, Informationssicherheit und Amtsgeheimnis – eingehalten werden und dass KI-Resultate kritisch geprüft werden. Generative KI ist demnach grundsätzlich als Arbeitshilfe zu verstehen, deren Ergebnisse einer menschlichen Kontrolle unterliegen müssen.

3.3.8. Strafrecht

Die strafrechtliche Beurteilung des Einsatzes von KI erfolgt auf der Grundlage des technologieneutralen Strafrechts und knüpft – unabhängig vom verwendeten Instrument – an tatbestandsmässiges menschliches Verhalten an. Erfasst werden dabei sowohl die klassischen Delikte gegen die Ehre (z. B. mittels Deepfake-Technologie) nach Art. 173 ff. des Schweizerischen Strafgesetzbuches (StGB) vom 21. Dezember 1937 (SR 311.0) oder gegen den Geheim- oder Privatbereich (Art. 179 ff. StGB), das unbefugte Beschaffen von Personendaten (Art. 179^{octies} StGB) oder der Identitätsmissbrauch (Art. 179^{novies} StGB). Darunter fallen aber auch Vermögensdelikte wie Betrug (Art. 146 StGB) oder Warenfälschung (Art. 155 StGB), wenn sich die Täterschaft der KI-Technologien bedient. Solange tatbestandsmässiges Handeln vorliegt, verbleibt die Verantwortung beim Menschen beziehungsweise. beim Täterkreis, der die Technologie nutzt[51].

Von besonderer praktischer Relevanz sind KI-gestützte Täuschungshandlungen im Sexualstrafrecht. Für Deepfakes sind insbesondere Art. 197 Abs. 4 und 5 StGB (qualifizierte Pornografie) einschlägig, welcher die Herstellung, den Besitz und die Verbreitung von pornografischem Material bestraft und dabei namentlich die Minderjährigen schützen will. Darunter fallen unter anderem auch Deepfakes, welche selbst ohne sexuelle Handlungen mit Minderjährigen zustande gekommen sind, aber mittels Datenbearbeitung generiert wurden (siehe hierzu auch Art. 5 Abs. 1 StGB)[52]

Auf dieser Grundlage richtet sich die Verantwortlichkeit weiterhin nach dem Schuldprinzip: Es gibt keine Strafe ohne Schuld. Die strafrechtliche Verantwortlichkeit knüpft weiterhin an die Schuldfähigkeit einer natürlichen Person. Sie erfasst deshalb keine Technologien wie beispielsweise ein KI-System. Ein originärer subjektiver Tatbestand für KI wird auch in der Lehre überwiegend verworfen. Daraus folgt, dass die Zurechnung und die Verantwortlichkeit typischerweise zwischen der Ebene des Nutzers und des Herstellers und gegebenenfalls des Halters (z. B. Halterhaftung nach SVG) von automatisierten oder autonom funktionierenden KI-Systemen verläuft. Kann jedoch eine Schädigung keiner natürlichen Person zugerechnet werden,

[51] BJ, Rechtliche Basisanalyse, S. 164.
[52] BJ, Rechtliche Basisanalyse, S. 165.

kommt die Verantwortlichkeit des Unternehmens (Art. 102 StGB) in Betracht. Zugleich deutet die Entwicklung auf einen «accountability shift» hin: Mit höherem Automatisierungsgrad rückt die Strafbarkeit zunehmend in Richtung Hersteller[53].

Im operativen Umgang mit KI-Systemen bestehen für Hersteller grundsätzlich dieselben Sorgfaltspflichten wie bei herkömmlichen technischen Produkten. Deren Konkretisierung kann je nach Systemart, Einsatzbereich und Gefährdung strafrechtlich geschützter Rechtsgüter variieren. Herausfordernd wird die Zurechnung insbesondere dort, wo Maschinen weitgehend automatisiert bis autonom handeln und algorithmisch determinierte Handlungen bisher menschliche Entscheidungen ersetzen – etwa in Medizin, Strassenverkehr oder modernen Waffensystemen. Mit zunehmender Komplexität der eingesetzten KI verstärken sich in der Praxis die Abgrenzungs- und Beweisprobleme. Lernfähige Systeme entwickeln sich autonom fort, Vorgänge sind nicht immer ex ante vorhersehbar und zuweilen ex post nicht vollständig transparent oder nachvollziehbar. Damit verschiebt sich die Schwierigkeit weg vom materiellen Recht hin zur Frage der Zurechenbarkeit bei der Rechtsdurchsetzung: Wo liegt der Fehler, wer hat ihn schuldhaft verursacht, waren Sorgfaltspflichtverletzungen ex ante erkenn- und vermeidbar (Blackbox-Problematik)?

Anschaulich zeigt dies das Beispiel des automatisierten Fahrens. Fahrzeuge übernehmen weitgehend die Steuerung. Die Beherrschungspflicht der Fahrzeuglenkenden bleibt, wird aber mit fortschreitender Automatisierung teilweise relativiert. Ein Verschulden ist zu bejahen, wenn trotz Pflicht, Möglichkeit und Zumutbarkeit ein gebotenes Eingreifen unterlassen wird.

Zusammenfassend bietet das materielle Strafrecht aufgrund seiner Technologieneutralität einen im Grundsatz geeigneten Rahmen für Vorsatz- und Fahrlässigkeitsdelikte im Kontext von KI. Massgeblich bleibt das Schuldprinzip und damit das vorwerfbare Verschulden im Einzelfall. Bei Fahrlässigkeit rückt die Frage ins Zentrum, ob Einsatz, Herstellung oder Inverkehrbringen als Sorgfaltspflichtverletzung oder als erlaubtes Risiko zu qualifizieren sind sowie ob einschlägige Sorgfaltspflichten und Fehlerquellen ex ante erkenn- und vermeidbar waren. Eine verschuldensunabhängige Kausalhaftung ist strafrechtlich weiterhin ausgeschlossen. In der Tendenz. Sektoriell präzisierte Sorgfaltspflichten – etwa im automatisierten Fahren – können punktuell Klarheit schaffen und zugleich Transparenz- und Rechenschaftsgrundsätze stärken[54].

3.4. Regulierungsansatz des Bundes

Die Schweiz hat am 27. März 2025 die «Rahmenkonvention des Europarates über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit» (KI-Konvention) ratifiziert. Der Bundesrat will bis Ende 2026 die notwendigen gesetzlichen Anpassungen erarbeiten und in die Vernehmlassung geben. Dabei möchte er sich an folgenden Punkten orientieren:

- In erster Linie sollen staatliche Akteure in den Geltungsbereich der KI-Konvention fallen.
- Wo Gesetzesanpassungen nötig sind, sollen diese möglichst sektorbezogen ausfallen. Eine allgemeine, sektorübergreifende Regulierung soll sich auf zentrale, grundrechtsrelevante Bereiche, wie beispielsweise den Datenschutz, beschränken.
- Neben der Gesetzgebung sollen auch rechtlich nicht verbindliche Massnahmen zur Umsetzung der Konvention erarbeitet werden, wozu auch Selbstdeklarationsvereinbarungen oder Branchenlösungen gehören sollen.

Im Vorfeld zur Ratifikation der KI-Konvention hatte der Bundesrat das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) und das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) beauftragt, eine Auslegeordnung zur

[53] BJ, Rechtliche Basisanalyse, S. 166.

möglichen Regulierung von KI zu erstellen, die dem Bundesrat als Grundlage für einen Grundsatz-entscheid zum künftigen schweizerischen Regulierungsansatz dient. Die Auslegeordnung wurde gleichzeitig mit einer Medienmitteilung des Bundesrats am 12. Februar 2025 publiziert.

Die Erstellung erfolgte innerhalb der Interdepartementalen Koordinationsgruppe EU-Digitalpolitik (IK EUDP). Als Grundlagen für die Erstellung der Auslegeordnung wurden vorab detaillierte Basisanalysen durchgeführt: eine rechtliche Basisanalyse, eine Analyse zu den Regulierungsaktivitäten in einzelnen Sektoren der Schweizer Wirtschaft und eine Analyse der KI-Regulierung in verschiedenen Ländern[55]. Zudem wurden externe Akteure aus Wirtschaft, Wissenschaft und Zivilgesellschaft über die Plattform Tripartite Suisse[56] in die Arbeiten miteinbezogen.

Die Länderanalyse des Bundesamts für Kommunikation (BAKOM) zeigt eine Vielfalt an Regulierungsansätzen ohne klar dominierenden Weg, mit nationalen KI-Strategien in vielen Staaten, aber nur wenigen bereits in Kraft stehenden KI-Spezialgesetzen ausserhalb der EU. Die Wahl zwischen horizontalen und sektoriellen Ansätzen ist international uneinheitlich, wobei vielfach risikobasierte Instrumente verfolgt werden[57].

Die sektorielle Analyse erhob bei 66 Bundesstellen 41 Rückmeldungen und identifizierte die Schwerpunkte Transparenz und Nachvollziehbarkeit, Schutz der Privatsphäre und des Datenschutzes, Vermeidung von Diskriminierung sowie Cybersicherheit. Die Relevanz und Gewichtung dieser Schwerpunkte variieren je nach Sektor, doch besteht ein breiter Konsens, dass ein sektorieller Regulierungsansatz aus rechtlichen und zeitlichen Gründen nicht ausreichend sei und deshalb der KI-Bereich im Grundsatz sektorübergreifend zu regulieren sei, auch nur, um divergierende, sektorielle Regulierungen zu verhindern[58].

Auf technischer Ebene konkretisieren sodann internationale Normierungsarbeiten die rechtlichen Rahmenbedingungen. Internationalen Organisationen wie IEC, ISO und ITU sowie IEEE erarbeiten Standards zu Terminologie, Governance, Risikomanagement, Cybersicherheit und ethische Überlegungen, welche auch für die Schweiz relevant sind. Die Standards sollen geeignete Leitlinien für eine verantwortungsvolle, sichere und vertrauenswürdige KI-Entwicklung bieten.

In der EU hat die Europäische Kommission das Europäische Komitee für Normierung (CEN) und das Komitee für elektrotechnische Normierung (CENELEC) beauftragt, technische Normen zur Unterstützung des AI Act zu entwickeln. Diese Standards betreffen Hochrisiko-KI-Systeme, Qualitätsmanagement, Konformitätsbewertung sowie zentrale Aspekte wie Risikomanagement, Datenqualität, Transparenz, menschliche Aufsicht, Robustheit und Cybersicherheit. Aufgrund ihres grenzüberschreitenden Charakters sind sie auch in der Schweiz zu beachten, so insbesondere in Bereichen wie Luftfahrt, Strassen- und Bahnverkehr. Die zuständigen Bundesstellen verfolgen diese Arbeiten eng oder wirken in Fachgremien mit, damit anschliessend Anpassungen von Verweisen auf technische Normen auch in die schweizerischen Gesetzen und Verordnungen aufgenommen werden können[59].

Für die Schweiz liegen bislang keine verlässlichen Zahlen zur Grösse und Bedeutung des KI-Marktes vor. Gleichwohl muss aber von einer erheblichen Betroffenheit unterschiedlichster

---

55 BAKOM, Auslegeordnung und Basisanalysen (https://www.bakom.admin.ch/de/kuenstliche-intelligenz; besucht am 5. März 2026).
56 BAKOM, Die Plateforme Tripartite Suisse für digitale Gouvernanz und künstliche Intelligenz (https://www.bakom.admin.ch/de/die-plateforme-tripartite-suisse-fuer-digitale-gouvernanz-und-kuenstliche-intelligenz; besucht am 5. März 2026).
57 BAKOM, Auslegeordnung, S. 6 f.
58 BAKOM, Auslegeordnung, S. 12 f.
59 BAKOM, Auslegeordnung, S. 13 f.

Wirtschaftsakteure ausgegangen werden. Start-ups, KMU und Grossunternehmen in Bereichen wie Medizinaltechnik, Mobilität, Maschinenindustrie und Unterhaltungselektronik wären von regulatorischen Massnahmen unmittelbar tangiert. Eine einheitliche Haltung der Wirtschaft zeichnet sich jedoch nicht ab. Vielmehr bestehen auf Seiten der Unternehmen heterogene Bedürfnisse und Erwartungen[60].

Mit Blick auf den AI Act der EU gilt es festzuhalten, dass Schweizer Unternehmen im EU-Binnenmarkt dessen Anforderungen bereits heute erfüllen müssen. Ein vom BAKOM im Mai 2024 initiierter Austausch sowie eine Befragung der Wirtschaft haben gezeigt, dass Marktzugangshürden unbedingt zu vermeiden sind, da die EU der wichtigste Absatzmarkt für Schweizer KI-Produkte und -Dienstleistungen bleibt. Gleichzeitig soll der Schweizer Markt offen und innovationsfreundlich ausgestaltet werden. Eine vollständige Übernahme des AI Acts wird in der Wirtschaft überwiegend kritisch beurteilt, da ein erheblicher bürokratischer Aufwand befürchtet wird. So hat sich beispielsweise Economiesuisse im bisherigen Prozess klar gegen eine KI-spezifische Gesetzgebung nach dem Vorbild des AI Act ausgesprochen[61].

Bevorzugt werden gezielte Anpassungen einzelner Gesetze, wobei mehrfach betont wurde, dass die Schweiz nicht übereilt handeln, sondern zunächst die Umsetzung in den EU-Mitgliedstaaten abwarten soll. Ebenso wird gefordert, dass ein «Swiss Finish», welcher über die Anforderungen der EU hinausgehen würde, vermieden wird[62].

Wirtschaftlich von Bedeutung ist das Abkommen über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA CH-EU) zwischen der Schweiz und der EU[63], das rund zwei Drittel des Handels mit Industrieerzeugnissen abdeckt. Zwölf der zwanzig im MRA CH-EU geregelten Produktesektoren fallen damit künftig unter den Anwendungsbereich des AI Acts, sobald diese Produkte KI-Bestandteile enthalten. Ab August 2027 treten zudem die neuen Vorgaben des AI Act für Hochrisiko-Systeme in Kraft. Dadurch können die Produkte in diesen zwölf Sektoren auch unter diese Vorgaben fallen, sofern sie risikoreiche KI-Komponenten enthalten. Damit drohen Schweizer Herstellern doppelte Konformitätsbewertungen nach dem MRA CH-EU und dem AI Act sowie unter anderem die Pflicht zur Benennung eines Bevollmächtigten in der EU. Dies wird für die betroffenen Unternehmen Mehraufwand und Kosten nach sich ziehen und für den Zugang von Schweizer KI-Produkten zum EU-Binnenmarkt zusätzliche Hindernisse bedeuten. Um neue technische Handelshemmnisse zu vermeiden, wären Anpassungen der schweizerischen Produktvorschriften sowie eine Erweiterung des MRA CH-EU notwendig[64].

Schliesslich wird in der Auslegeordnung des BAKOM hervorgehoben, dass ein innovationsfreundliches Umfeld entscheidend bleibt, um die Wettbewerbsfähigkeit der Schweiz im KI-Bereich zu sichern. Der Bundesrat will bis spätestens Mitte 2026 einen Bericht vorlegen, der bestehende und neue Förderinstrumente für KI sowie die Anbindung an das Digital Europe Programme der EU darstellt. Bereits heute setzen Hochschulen und Institutionen wie der ETH-Bereich und die Akademien der Wissenschaften zentrale Schwerpunkte auf Digitalisierung und KI. Mit der «Swiss AI»-Initiative von ETH Zürich und EPFL sowie der Innosuisse-Flagship-Initiative im Bereich KI und Gesundheit werden zusätzliche Impulse für die Stärkung der Schweiz als innovativer und international relevanter KI-Standort erwartet[65].

---

60 BAKOM, Auslegeordnung, S. 14.
61 BAKOM, Auslegeordnung, S. 14.
62 BAKOM, Auslegeordnung, S. 15.
63 Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die gegenseitige Anerkennung von Konformitätsbewertungen vom 21. Juni 1999 (SR 0.946.526.82).
64 BAKOM, Auslegeordnung, S. 15 f.
65 BAKOM, Auslegeordnung, S. 16.

Der Bundesrat hatte bereits wiederholt dargelegt, welche Prinzipien bei der Regulierung neuer Technologien zu beachten sind. Diese Grundsätze lassen sich auch auf den Umgang mit KI anwenden. Vorrangig ist, dass der Staat innovationsfreundliche Rahmenbedingungen für Wirtschaft und Forschung schafft und dabei die Rechtsordnung wahrt, während Markt und Gesellschaft darüber entscheiden, welche Technologien sich durchsetzen. Gleichzeitig sind die Grundrechte als elementare Werte des Rechtsstaats zu achten und in allen Regulierungsüberlegungen zu berücksichtigen. Die Schweiz soll dabei ihren bewährten Rechtsrahmen nicht grundsätzlich infrage stellen, ihn aber dort anpassen, wo Rechtslücken oder Hindernisse bestehen. Angestrebt wird ein prinzipienbasierter und technologieneutraler Ansatz, der jedoch im Bedarfsfall Ausnahmen zulässt und wettbewerbsneutral ausgestaltet wird. Eingriffe sollen aus Effizienzgründen nur erfolgen, wenn sie zu einer Verbesserung der Markteffizienz führen. Zudem sollen die Behörden eine offene Haltung gegenüber neuen Technologien einnehmen und den regelmässigen Dialog mit allen betroffenen Akteuren pflegen[66].

Der bestehende Rechtsrahmen der Schweiz wird als flexibel eingeschätzt und kann für neuartige Entwicklungen genutzt werden. Bereits heute bietet er für viele Fragestellungen im KI-Kontext eine Orientierung. KI gilt als Basistechnologie mit breitem Anwendungsfeld und hoher Produktivitätswirkung, die Chancen aber auch Risiken auf individueller wie gesamtgesellschaftlicher Ebene birgt. Während viele Menschen in der Schweiz KI bereits im Alltag nutzen – etwa durch Sprachassistenten oder Gesundheits-Apps – bleibt die Haltung gegenüber dieser Technologie ambivalent. Ein sicherer Rechtsrahmen kann das Vertrauen in KI stärken, indem er Schutz vor missbräuchlichen Anwendungen gewährleistet und den Menschen ermöglicht, ihre Rechte wirksam wahrzunehmen[67].

Besondere Bedeutung kommt der internationalen Offenheit der Schweiz zu. Als mittelgrosse, offene Volkswirtschaft mit kleinem Binnenmarkt ist sie auf den internationalen Handel angewiesen und strebt an, technische Handelshemmnisse zu vermeiden oder abzubauen. In der Legislaturplanung 2023 – 2027 hebt der Bundesrat hervor, dass die Innovationskraft des Landes eine zentrale Rolle für den Wohlstand spielt. Die Schweiz zählt seit Jahren zu den international führenden Innovationsstandorten. Regulierungsansätze müssen daher so gestaltet sein, dass sie neben dem Schutz der Gesellschaft auch die internationale Anschlussfähigkeit und Wettbewerbsfähigkeit sichern[68].

Vor diesem Hintergrund werden drei übergeordnete Regulierungsziele identifiziert:

- Stärkung des Innovationsstandorts Schweiz, indem Regulierung den Akteuren Raum zur Entfaltung gibt, den Zugang zu Märkten und Forschungsräumen unterstützt und den Import von Technologien erleichtert.
- Wahrung des Grundrechtsschutzes, inklusive der Wirtschaftsfreiheit, durch eine Regulierung, die sicherstellt, dass Grundrechte mit den technologischen Entwicklungen Schritt halten.
- Stärkung des Vertrauens der Bevölkerung in KI, was voraussetzt, dass KI-Systeme zuverlässig, robust und vertrauenswürdig sind, dass Transparenz, Nachvollziehbarkeit und Erklärbarkeit von Prozessen gewährleistet wird und die Bevölkerung befähigt wird, KI-Systeme kompetent einzusetzen.

Diese Ziele bilden die Grundlage für die Diskussion künftiger Regulierungsansätze[69].

---

66 BAKOM, Auslegeordnung, S. 19.
67 BAKOM, Auslegeordnung, S. 19 f.
68 BAKOM, Auslegeordnung, S. 20.
69 BAKOM, Auslegeordnung, S. 20.

Aufbauend auf den dargestellten Regulierungsprinzipien und -zielen werden verschiedene Regulierungsansätze für den Umgang mit KI in der Schweiz skizziert. Sie unterscheiden sich hinsichtlich ihres Eingriffsgrads und der institutionellen Konsequenzen, bauen aber konzeptionell aufeinander auf. Allen Ansätzen ist gemeinsam, dass sie nicht bis ins Detail ausgearbeitet sind, sondern einen Orientierungsrahmen darstellen, der je nach Entscheid des Bundesrats weiter vertieft werden müsste.

Ein erster Ansatz sieht die Fortführung bestehender themen- und sektorspezifischer Regulierungsaktivitäten vor. Anpassungen würden in den zuständigen Fachämtern nach sektoralen Bedürfnissen vorgenommen, ohne dass eine koordinierte übergeordnete Regulierung angestrebt wird. Damit bliebe es bei punktuellen Anpassungen einzelner Gesetze, Verordnungen oder Richtlinien. Vorteile dieses Modells liegen in der gezielten Adressierung von Herausforderungen innerhalb einzelner Sektoren. Gleichzeitig birgt es das Risiko von Fragmentierung, unterschiedlichen Lösungen, Rechtsunsicherheit und Lücken bei Querschnittsthemen wie Transparenz oder Grundrechtsschutz. Institutionell wären keine neuen Strukturen erforderlich. Bestehende Aufsichtsbehörden würden ihre Zuständigkeiten bei Bedarf ausweiten[70].

Ein zweiter Ansatz bestünde in der Ratifikation der KI-Konvention des Europarats. Sie stellt das erste verbindliche internationale Abkommen zu KI dar und verpflichtet die Vertragsstaaten insbesondere in den Bereichen Grundrechtsschutz, Transparenz, Risiko- und Folgenabschätzung sowie Aufsicht. Für die Schweiz hätte die Ratifikation Signalwirkung im Hinblick auf die internationale Glaubwürdigkeit und würde ein gleichwertiges Schutzniveau sicherstellen. Die Umsetzung könnte minimal oder weitergehend erfolgen. Eine Minimalumsetzung würde nur die notwendigsten Anpassungen im öffentlichen und einem begrenzten Kreis privater Sektoren erfordern, etwa Registrierungspflichten für staatlich eingesetzte KI-Systeme oder punktuelle Ergänzungen im Datenschutzrecht. Eine weitergehende Umsetzung könnte umfassendere Transparenzpflichten, eine Ausweitung des Diskriminierungsschutzes und erweiterte Aufsichtsbefugnisse beinhalten, teilweise auch mit neuen institutionellen Strukturen. Beide Varianten würden jedoch einen koordinierten Ansatz beim Bund erforderlich machen, um sektorübergreifende Herausforderungen kohärent zu adressieren[71].

Ein dritter Ansatz würde über die Ratifikation der KI-Konvention hinausgehen und eine Umsetzung in Anlehnung an den AI Act vorsehen. Dies entspräche einer produktbezogenen, risikobasierten Querschnittsregelung, die eine hohe Kompatibilität mit den europäischen Vorgaben herstellen würde. KI-Systeme würden in Risikoklassen eingeteilt, wo für abgestufte Pflichten gälten. Private wie staatliche Akteure wären gleichermassen betroffen und müssten Anforderungen zu Datenqualität, Dokumentation und Risikobewertung erfüllen. Eine solche Regulierung könnte in einem neuen KI-Gesetz gebündelt werden, um Einheitlichkeit und Rechtssicherheit zu schaffen. Der Ansatz würde zwar zu einer hohen Regulierungsdichte führen, zugleich aber den Zugang zum europäischen Binnenmarkt erleichtern – vorausgesetzt, das MRA CH-EU würde entsprechend erweitert. Ohne eine Anpassung des MRA CH-EU bliebe der Marktzugang hingegen beschränkt[72].

Neben diesen drei Ansätzen werden zusätzliche Instrumente diskutiert, die unabhängig vom gewählten Modell eingesetzt werden könnten. Hierzu gehören regulatorische Sandboxen, die es erlauben, Pilotprojekte unter erleichterten Rahmenbedingungen durchzuführen. Sie fördern Innovation und helfen, regulatorische Hürden sichtbar zu machen. Ergänzend könnten risikobasierte Regulierungen, Innovations Hubs und branchenspezifische Verhaltenskodizes eingesetzt

[70] BAKOM, Auslegeordnung, S. 21 f.
[71] BAKOM, Auslegeordnung, S. 22 ff.
[72] BAKOM, Auslegeordnung, S. 24 ff.

werden. Diese Instrumente eröffnen Chancen, bergen aber auch Risiken, etwa durch mögliche Wettbewerbsverzerrungen, die im Vorfeld sorgfältig abzuwägen wären[73].

Aufbauend darauf hat der Bundesrat am 12. Februar 2025 klargestellt, dass die KI-Konvention formal in Schweizer Recht übernommen werden soll, primär für staatliche Akteure, mit gezielten sektorbezogenen Anpassungen und sektorübergreifenden Regeln nur für zentrale grundrechtsrelevante Bereiche. Zusätzlich sind nicht verbindliche Instrumente wie Branchenlösungen und Selbstdeklarationen vorgesehen; Wirtschaft, Wissenschaft und weitere Anspruchsgruppen werden einbezogen. Das EJPD erarbeitet bis Ende 2026 eine Vernehmlassungsvorlage mit Schwerpunkten Transparenz, Datenschutz, Nichtdiskriminierung und Aufsicht. UVEK, EJPD, EDA und WBF entwickeln parallel einen Plan für nicht gesetzliche Massnahmen und sichern Kompatibilität mit wichtigen Handelspartnern. Am 12. Dezember 2025 nahm der Bundesrat zudem einen Umsetzungsplan und ein Konzept zur Stärkung des Kompetenznetzwerks für KI (CNAI) in der Bundesverwaltung zur Kenntnis. Vorgesehen sind Erfassung des KI-Potenzials in den Departementen, Leitlinien für den internen KI-Einsatz, Ausbau von Kompetenzen und Austauschformaten sowie institutionelle Koordination durch Übertragung der CNAI-Verantwortung an die Bundeskanzlei. Diese organisatorischen Schritte stärken Transparenz, Rechtssicherheit und Vertrauen innerhalb der Verwaltung[74, 75].

3.5. Regulierung im Kanton Zug

3.5.1. Auslegeordnung der Kantone zur Regelung von KI[76]

Die Konferenz der Kantonsregierungen (KdK) befragte im Frühling 2025 alle Staatskanzleien zum Umgang mit KI. Damals bestanden kaum übergeordnete kantonale KI-Regulierungen. Punktuelle Datenschutzanpassungen gab es in Jura, Neuenburg und St. Gallen; in Genf, Schwyz und Zürich laufen Revisionen zur Aufnahme allgemeiner KI-Bestimmungen; Solothurn verfügt als einziger Kanton über eine sektorspezifische Regulierung. Nahezu alle Kantone haben Leitlinien oder Merkblätter für den KI-Umgang in ihren Verwaltungen erlassen. Die Auslegeordnung zeigt, dass die Kantone Ratifikation und bundesrätlichen Umsetzungsansatz grundsätzlich unterstützen und zugleich anerkennen, dass Umsetzung Auswirkungen auf kantonaler Ebene haben und gesetzliche Anpassungen oder neue Regelungen erforderlich machen kann.

3.5.2. Einsatzmöglichkeiten von KI in der kantonalen Verwaltung und Justiz

Die Ratifizierung der KI-Konvention beeinflusst die Kantone; sie müssen prüfen, wo in ihrem Zuständigkeitsbereich Gesetzesanpassungen notwendig sind und ob eine allgemeine sektorübergreifende Regulierung angezeigt ist. Einsatzfelder von KI finden sich vor allem dort, wo Prozesse entlastet, Effizienz gesteigert und Qualität verbessert werden können: wiederkehrende strukturierte Tätigkeiten ohne Ermessensspielraum, wiederkehrende ähnliche Informationsanfragen, Massenverwaltung mit grossen strukturierten Datenmengen, Prognosen, intelligente Informationsdurchsuchung, anspruchsgruppengerechte Verwaltungsdienstleistungen sowie Informationssicherheit und Cyberschutz.

Mögliche Anwendungen sind insbesondere Textgeneratoren wie Copilot, Übersetzungsdienste wie DeepL, Schreibassistenten wie DeepL Write, Text-, Sprach- oder Bilderkennung, etwa Speech-to-Text bei Anhörungen oder Geodatenanalyse anhand von Satellitenbildern, Chatbots

---

73 BAKOM, Auslegeordnung, S. 26 f.

74 Medienmitteilung des Bundesrates vom 12. Februar 2025, KI-Regulierung: Bundesrat will Konvention des Europarates ratifizieren (https://www.news.admin.ch/de/nsb?id=104110; besucht am 5. März 2026).

75 Medienmitteilung des Bunderates vom 12. Dezember 2025, Bund plant gezielte Massnahmen für den Einsatz von KI in der Bundesverwaltung und stärkt Koordination (https://www.news.admin.ch/de/newnsb/nTc28qni5hdpzQ0tH6RGa; besucht am 5. März 2026).

76 KdK-Bericht vom 19. Dezember 2025, Die Regelung von Künstlicher Intelligenz in den Kantonen: eine Auslegeordnung (https://kdk.ch/fileadmin/redaktion/themen/aktuelle_Geschaefte/KI-Auslegeordnung-2025.DE.pdf; besucht am 5. März 2026).

sowie KI-basierte Informationssicherheitslösungen zur Erkennung von Bedrohungen, Muster- und Anomalieanalyse und automatisierter Reaktion. Weitere Einsatzgebiete sind die Automatisierung von Massenverfahren wie Prämienverbilligungen oder Steuerverfahren, Vorhersagen künftiger Delikte und Deliktsorte anhand von Kriminalitätsdaten, Durchsuchung grosser Datenmengen nach korrespondierenden Namen, Adressen oder Kontonummern im Bereich Wirtschaftskriminalität, Deepfake-Detektion, Videoanalyse, automatische Fahrzeugfahndung und Verkehrsüberwachung, Fallscreening im Justizvollzug zur Entscheidung über vertiefte risikoorientierte Einzelfallanalysen sowie Bedrohungserkennung und -analyse im Netzwerkverkehr, Benutzerverhalten und anderen Daten, namentlich zur Erkennung von Malware, Phishing oder Ransomware[77].

3.5.3. Kantonaler Regulierungsbedarf

Die KI-Konvention verpflichtet die Schweiz, Grundrechte, Demokratie und Rechtsstaatlichkeit auch digital zu sichern. Dies betrifft Kantone, soweit Regelungsbereiche in deren Kompetenz liegen. Der Kanton Zug wird seine Rechtsordnung prüfen und bei Bedarf weiterentwickeln müssen, um bundesrechtliche und völkerrechtliche Anforderungen kohärent umzusetzen. Zunächst sind jedoch die bis Ende 2026 vom EJPD zu erarbeitenden gesetzlichen Grundlagen zur Umsetzung der KI-Konvention abzuwarten. Bis zu deren Inkrafttreten bilden die unter Ziffer 3.3 dargestellten nationalen und kantonalen Regelungen sowie rechtsstaatlichen Grundsätze einen ausreichenden Rahmen für den KI-Einsatz.

Parallel laufen koordinierte kantonale Vorbereitungsarbeiten. Der Leitende Ausschuss der Konferenz der Kantonsregierungen (KdK) vergab am 13. Februar 2026 einen externen Auftrag an das *electronic Public Institutions and Administrations Research Forum (e-PIAF)* der Juristischen Fakultät der Universität Basel. Unter der Leitung von Prof. Dr. Nadia Braun Binder und in Zusammenarbeit mit AlgorithmWatch.ch werden konzeptionelle und rechtliche Grundlagen für die kantonale Umsetzung der KI-Konvention erarbeitet. Der Auftrag umfasst Umsetzungskonzepte und Musterregelungen zu Transparenz, Nachvollziehbarkeit, Diskriminierungsschutz und Aufsicht beim Einsatz von KI-Systemen in kantonalen Verwaltungen, namentlich auch im Zusammenhang mit Verzeichnissen von KI-Systemen sowie Folgenabschätzungen, sowie Varianten für Aufsichtsprozesse und -strukturen. Ergebnisse werden voraussichtlich bis Ende 2026 vorliegen.

Vor diesem Hintergrund ist mittelfristig zu prüfen, ob und in welcher Form ein eigenständiger kantonaler Rechtsrahmen erforderlich ist; die weiteren Entwicklungen auf Ebene KdK und Bund sind abzuwarten. Bereits heute kann die organisatorische Zuständigkeit und Governance geklärt werden. KI ist ein Querschnittsthema in IT, Infrastruktur, Recht, Datenschutz, Kommunikation und Ethik. Zweckmässig erscheint eine klare Rollenteilung: strategische Steuerung durch den Regierungsrat, technische Verantwortung für Plattform, Architektur und Betrieb beim AIO sowie fachliche Verantwortung bei Direktionen, Staatskanzlei und Gerichten. Der Regierungsrat verfolgt die Umsetzungsarbeiten auf Bundes- und Kantonsebene laufend und leitet notwendige Anpassungen des kantonalen Rechts zu gegebener Zeit ein.

4. Postulat von Joëlle Gautier, Jill Nussbaumer, Etienne Schumpf, Alex Haslimann und Michael Felber betreffend Schaffung von Grundlagen für die erfolgreiche Anwendung von KI-Modellen im öffentlichen Sektor (# 3896)

4.1. Ausgangslage

[77] ZH-Schlussbericht, S. 24 ff.

Der Regierungsrat anerkennt die zunehmende Bedeutung von Anwendungen der KI für die öffentliche Verwaltung. KI-Systeme können zur Effizienzsteigerung, zur Qualitätsverbesserung von Dienstleistungen sowie zur Entlastung der Mitarbeitenden beitragen. Gleichzeitig stellen sie besondere Anforderungen an den Schutz der Grundrechte, an Transparenz, Nachvollziehbarkeit sowie an Datenschutz und Informationssicherheit.

4.2. Rechtliche Grundlagen für die Implementierung von KI

Für die Implementierung von KI im Kanton Zug ist zentral, dass die bestehenden nationalen und kantonalen Rechtsgrundlagen eingehalten werden. Dabei ist zu berücksichtigen, dass zwischen Automatisierung und künstlicher Intelligenz zu unterscheiden ist, wobei sich in beiden Fällen insbesondere Fragen des Datenschutzes und der Datensicherheit stellen. Die Abgrenzung ist in der Praxis jedoch nicht immer trennscharf möglich, da KI-Anwendungen häufig auf automatisierten Prozessen aufbauen beziehungsweise diese erweitern. Eine isolierte Betrachtung erscheint daher nur bedingt zweckmässig. Vor diesem Hintergrund kommt den bestehenden rechtlichen Rahmenbedingungen zentrale Bedeutung zu, wobei insbesondere das kantonale Datenschutzgesetz (DSG, BGS 157.1; vgl. Ziff. 3.3.3) massgeblich ist. Darüber hinaus verlangt die Verordnung über die Informationssicherheit von Personendaten (VIP, BGS 157.12), dass die Behörden geeignete technische und organisatorische Massnahmen umsetzen, um die Sicherheit der bearbeiteten Daten zu gewährleisten. Für KI-Systeme bedeutet dies insbesondere, dass Fragen wie Datenqualität, Zugriffskontrolle, Schutz vor Manipulationen sowie eine klare Verantwortungszuordnung von Beginn weg berücksichtigt werden müssen.

Bei KI-Anwendungen in hoheitlichen Verfahren ist zudem das Verwaltungsrechtspflegegesetz (VRG, BGS 162.1) einschlägig. Verfahrensgarantien wie Anspruch auf rechtliches Gehör (§ 7 ff. VRG) und die Begründungspflicht von Verfügungen (§ 28 VRG) gelten uneingeschränkt auch bei automatisierten oder teilautomatisierten Entscheiden. Damit ist sicherzustellen, dass die betroffenen Personen ihre Rechte wahren können und die Entscheidungsfindung für sie nachvollziehbar bleibt. Dies deckt sich mit den bereits hervorgehobenen Überlegungen, wonach ein Einsatz von KI in der Verwaltung nur dort erfolgen darf, wo rechtsstaatliche Garantien gewahrt sind und die Betroffenen nicht den intransparenten Abläufen eines Systems ausgeliefert werden.

Der Kanton Zug verfügt mit dem kantonalen Datenschutzgesetz (DSG), der Verordnung über die Informationssicherheit von Personendaten (VIP) sowie dem Verwaltungsrechtspflegegesetz (VRG) über zentrale Rechtsinstrumente, die den Einsatz von KI grundsätzlich rechtlich abdecken. Neue materielle Datenschutzvorschriften sind dabei nicht erforderlich, da die bestehenden Erlasse technologieneutral ausgestaltet sind.

4.3. Technische und organisatorische Umsetzung von Datenschutzvorgaben

Entscheidend ist, dass datenschutzrechtliche Vorgaben technisch und organisatorisch wirksam umgesetzt werden. Ausgangspunkt bilden DSG und VIP. Bereits bei Entwicklung und Einführung von KI-Anwendungen sind geeignete Schutzmassnahmen vorzusehen, namentlich Verschlüsselung besonders schützenswerter Daten, sichere Speicher- und Übertragungsverfahren, Gewährleistung der Datenintegrität sowie Zugriffs- und Berechtigungskonzepte.

Organisatorisch braucht es klare Verantwortlichkeiten, regelmässige Risikoanalysen, DSFA bei KI-Einsatz in sensiblen Bereichen und regelmässige Überprüfung der Sicherheitsstandards. Besondere Aufmerksamkeit verlangt die Datenqualität, weil falsche, unvollständige oder verzerrte Daten systematische Fehlentscheide verursachen können und damit datenschutzrechtlich wie rechtsstaatlich problematisch sind. Transparenz und Nachvollziehbarkeit müssen

dokumentieren und überprüfbar machen, nach welchen Kriterien KI-gestützte Datenbearbeitung erfolgt. Dies stärkt Informationssicherheit und Vertrauen. Die technischen und organisatorischen Massnahmen bilden das Fundament eines datenschutzkonformen KI-Einsatzes; DSG und VIP geben verbindliche Regelwerke vor.

4.4. Schulung und Sensibilisierung

Der Einsatz von KI-Tools erfordert eine angemessene Schulung und Sensibilisierung der Mitarbeitenden der kantonalen Verwaltung, insbesondere im Hinblick auf den Datenschutz sowie die Einhaltung von Geheimhaltungspflichten (Amtsgeheimnis). Dies bildet eine wesentliche Voraussetzung für einen rechtmässigen und sicheren Einsatz von KI in der Verwaltung.

4.5. Technische und organisatorische Massnahmen für eine sichere Beschaffung von KI-Anwendungen

Bei KI ist nicht nur die Funktionalität, sondern auch die Einhaltung von Transparenz-, Datenschutz- und Sicherheitsstandards von Beginn an sicherzustellen. Dies verlangt, dass entsprechende Anforderungen bereits im Beschaffungsprozess verbindlich vorgegeben und vertraglich abgesichert werden. Zu beschaffenden Systeme müssen mit den kantonalen Vorgaben zur Datensicherheit und Informationssicherheit kompatibel sein. Anbieter müssen nachweisen, dass ihre Lösungen über wirksame Schutzmechanismen verfügen, dass die Datenhaltung den kantonalen Sicherheitsstandards entspricht und dass die Entscheidungsprozesse der Systeme nachvollziehbar dokumentiert sind. Damit wird gewährleistet, dass die Verwaltung auch nach der Einführung jederzeit in der Lage bleibt, ihrer Verantwortung gegenüber den betroffenen Personen gerecht zu werden.

Die internationale Regulierungspraxis zeigt, dass diese Anforderungen auch ausserhalb des Kantons Zug zunehmend verankert werden. So verpflichtet der AI Act der EU Anbieter von Hochrisiko-KI-Systemen dazu, umfassende Anforderungen an Risikomanagement, Datenqualität, Nachvollziehbarkeit, Dokumentation und Transparenz einzuhalten. Auch die KI-Konvention des Europarats über KI, Menschenrechte, Demokratie und Rechtsstaatlichkeit betont die Notwendigkeit, bereits im gesamten Lebenszyklus von KI-Systemen Schutzmassnahmen gegen Risiken für Grundrechte vorzusehen – wozu ausdrücklich auch die Phase der Beschaffung und Einführung gehört. Diese internationalen Vorgaben bilden wichtige Orientierungspunkte für den Kanton Zug, auch wenn sie (noch) nicht unmittelbar gelten.

4.6. Transparenzprinzip

Die Nachvollziehbarkeit von Entscheidungen ist eine Grundvoraussetzung für die Legitimität des staatlichen Handelns. Wird KI in der Verwaltung eingesetzt, darf dies nicht dazu führen, dass die Entscheidungsfindung für die betroffenen Personen undurchsichtig oder unverständlich wird. Vielmehr muss jederzeit ersichtlich bleiben, auf welcher Grundlage ein Entscheid getroffen wurde und welche Faktoren dabei berücksichtigt worden sind.

Das Verwaltungsrechtspflegegesetz (VRG, BGS 162.1) verpflichtet die Behörden in § 7 ff. zur Wahrung des rechtlichen Gehörs und in § 28 zur Begründungspflicht von Verfügungen. Diese Garantien gelten auch dann, wenn Entscheide teilweise oder vollständig durch KI-Systeme vorbereitet oder unterstützt werden. Eine formelhafte oder pauschale Begründung genügt nicht; vielmehr muss der Entscheid so erläutert werden, dass er für eine durchschnittliche betroffene Person verständlich bleibt.

Die Transparenzanforderungen betreffen nicht nur die technische Funktionsweise der Systeme, sondern auch die organisatorische Ebene. Zuständigkeiten, Abläufe und Kontrollmechanismen sind zu dokumentieren, damit klar bleibt, wer für einen Entscheid verantwortlich ist und wie mögliche Fehler korrigiert werden.

Das Transparenzprinzip ist eine tragende Säule für den rechtmässigen Einsatz von KI im Kanton Zug. Die bestehenden Grundlagen im VRG, im DSG und in der VIP bieten hierfür die rechtlichen Leitplanken. Entscheidend ist jedoch, dass sie in der Praxis konsequent angewendet werden. Entscheidungen müssen verständlich begründet, Verantwortlichkeiten klar geregelt und Abläufe überprüfbar bleiben. Nur so kann sichergestellt werden, dass der Einsatz von KI das Vertrauen in das staatliche Handeln stärkt und nicht untergräbt.

Der Umfang der Transparenzpflichten ist dabei differenziert zu betrachten. Der Einsatz von KI-Tools ausschliesslich zur Recherche stellt grundsätzlich eine interne Arbeitsweise dar und ist nicht offenzulegen. Dies ist vergleichbar mit der Wahl von Suchmaschinen, Suchbegriffen oder juristischen Datenbanken im Rahmen der Informationsbeschaffung. Eine Offenlegung wird hingegen erforderlich, wenn der Einsatz von KI über blosse Recherche- und Unterstützungstätigkeiten hinausgeht und entscheidrelevante Funktionen übernimmt oder in die eigentliche Entscheidfindung einbezogen wird. In diesen Fällen ist sicherzustellen, dass für die betroffenen Personen erkennbar ist, inwiefern KI-Systeme den Entscheid beeinflussen.

4.7. Fazit

Handlungsbedarf besteht aktuell im Kanton Zug derzeit ausschliesslich im Bereich des Transparenzprinzips gemäss § 4 Abs. 1 Bst. c DSG. Der Regierungsrat schlägt vor, dass das Amt für Informatik und Organisation (AIO) ein entsprechendes Projekt aufnimmt mit dem Ziel eine Liste jener Anwendungen zu publizieren, bei denen in der kantonalen Verwaltung KI eingesetzt wird.

Im Übrigen erachtet es der Regierungsrat als wesentlich, kein überhastetes Vorgehen zu wählen. Auch wenn sich KI-Technologien rasch weiterentwickeln, verfügt der Kanton Zug bereits heute über tragfähige rechtliche Grundlagen, welche den Einsatz von KI grundsätzlich abdecken. Diese sollen sorgfältig genutzt und weiterentwickelt werden, anstatt vorschnell neue Regelungen zu schaffen.

Der Regierungsrat teilt zudem die Einschätzung der Kantone, wonach die Ratifikation der KI-Konvention sowie der vom Bundesrat vorgeschlagene Umsetzungsansatz grundsätzlich zu unterstützen sind. Gleichzeitig ist anerkannt, dass deren Umsetzung Auswirkungen auf die kantonale Ebene haben kann und gegebenenfalls eine Weiterentwicklung bestehender gesetzlicher Grundlagen erforderlich macht. Vor diesem Hintergrund beabsichtigt der Regierungsrat, die weiteren Entwicklungen auf Bundes- und internationaler Ebene aufmerksam zu verfolgen und allfällige Anpassungen koordiniert, verhältnismässig und auf konkrete Erfahrungen aus der Praxis abgestützt vorzunehmen.

5. Anträge

Gestützt auf die vorstehenden Ausführungen beantragen wir Ihnen,

1. die Berichts-Motion von Esther Monney und Thomas Werner betreffend künstliche Intelligenz (KI) im Dienste des Kantons Zug: Rechtliche Grundlagen für den Einsatz in Verwaltung, Justiz und Polizei (Vorlage Nr. 3872 - 18020)
   a) erheblich zu erklären,
   b) vom vorliegenden Bericht des Regierungsrats Kenntnis zu nehmen und
   c) die Berichts-Motion als erledigt abzuschreiben.

2. das Postulat von Joëlle Gautier, Jill Nussbaumer, Etienne Schumpf, Alex Haslimann und Michael Felber betreffend Schaffung von Grundlagen für die erfolgreiche Anwendung von KI-Modellen im öffentlichen Sektor (Vorlage Nr. 3896.1 - 18086) im Sinne von Ziffer 4.6 teilerheblich zu erklären und als erledigt abzuschreiben.

Zug, 9. Juni 2026

Mit vorzüglicher Hochachtung
Regierungsrat des Kantons Zug

Der Landammann: Andreas Hostettler

Der Landschreiber: Tobias Moser

60/sm