

# AI-Systeme und Datenschutz-Compliance

AI-Systeme führen zu neuen rechtlichen Herausforderungen in vielen Bereichen. Besonders bedeutsam ist die Einhaltung des Datenschutzrechts. Unternehmen müssen deshalb ihre Datenschutz-Compliance verstärken.



Rolf H. Weber  
Prof. Dr. iur. Rechtsanwalt

## 1. Ausgangslage

AI-Systeme zeichnen sich dadurch aus, dass eine Umwandlung der eingegebenen Daten in Zahlen stattfindet. Datenschutzrechtlich erheblich ist dabei, ob Personendaten erfasst werden oder ob vorhandene Daten gestützt auf vielfältige Analysen gewisse Personen bestimmbar machen. Solange ein AI-System «lediglich» Sachdaten oder anonymisierte (pseudonymisierte) Daten verwendet, erscheint die Datenschutzproblematik als überblickbar, selbst wenn wegen der Weiterentwicklungen durch selbstlernende Algorithmen, die aus öffentlichen Daten auch personenbezogene Informationen in das Modell einzufügen vermögen, neue rechtliche Herausforderungen nicht auszuschliessen sind.

## 2. Grundsätze des Datenschutzrechts

Das Datenschutzrecht normiert die Bearbeitung von Personendaten in einer umfassenden Weise. Aus diesem Grunde ist es unumgänglich, dass AI-Systeme eine Ausgestaltung aufweisen, die es erlaubt, den Datenschutz-Anforderungen angemessen Genüge zu tun. Insbesondere sind die bekannten Datenbearbeitungsprinzipien einzuhalten. Um die Vorgaben an eine rechtmässige Datenbearbeitung und an die Gewährleistung der Datensicherheit gesetzeskonform einzuhalten, kommen Anbieter und Betreiber von AI-Systemen deshalb nicht umhin, der Compliance im Unternehmen ausreichend Beachtung zu schenken.

Ein besonderes Problemfeld betrifft die automatisierten Einzelentscheidungen; die betroffene Person darf nicht einem solchen Verfahren ausgesetzt sein, wenn die Entscheidung ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Ein für AI-Systeme besonders relevantes Problem betrifft die Tatsache, dass gemäss Wortlaut «ausschliesslich» automatisierte Datenbearbeitungen betroffen sind. Beim Profiling mag diese Voraussetzung erfüllt sein, nicht aber in denjenigen Fällen, die ein nicht automatisiertes Monitoring in der Form einer Plausibilitätsprüfung vorsehen. Die heutige Mehrheitsmeinung will zutreffend nicht allein auf das «Können» der Beeinflussung einer Entscheidung abstellen, sondern darauf, ob eine Überprüfung durch eine natürliche Person, die zudem rechtlich und faktisch in der Lage wäre, den maschinell getroffenen Entscheid umzustossen, tatsächlich erfolgt.

Das Ausmass der Datenschutz-Herausforderungen hängt zudem von der «Kontrolle» der verwendeten Infrastrukturen ab, d. h. von der Frage, ob eine eigene oder eine fremde Infrastruktur verwendet wird. Datenschutzrechtlich hat die Verwendung der eigenen Infrastruktur den Vorteil, dass es weder zu einer Datenbekanntgabe an Dritte noch zu einem grenzüberschreitenden Datenfluss ins Ausland kommt, doch ist deren Betreiber für die Wahrung der IT-Sicherheit verantwortlich.

## 3. Datenschutz-Compliance: Checkliste

Compliance bedeutet, dass die unternehmerischen Tätigkeiten mit den geltenden rechtlichen Rahmenbedingungen in Einklang stehen müssen. Im Lichte der immer komplexeren Vorgaben lassen sich eine Vielzahl an Massnahmen in Betracht ziehen. Insbesondere haben Unternehmen ein Compliance-Management-System zwecks Vermeidung von Fehlverhalten, zur Aufdeckung von Fehlverhalten und zur angemessenen Sanktionierung im Falle aufgedeckten Fehlverhaltens einzurichten.

Angesichts der nicht zu vernachlässigenden Rechtsunsicherheiten erscheint es als sinnvoll, wenn sich Anbieter und Betreiber von AI-Systemen, die Personendaten verarbeiten, eine Checkliste bereitlegen, um die datenschutzrechtlichen Herausforderungen sachgerecht zu erfüllen:

- Verarbeitet das AI-System auch Personendaten?
- Ist die Funktionsweise des AI-Systems nachvollziehbar?
- Wird der Grundsatz der Datenminimierung eingehalten?
- Ist die datenschutzrechtliche Rollenverteilung klar festgelegt?
- Nimmt das AI-System automatisierte Einzelentscheidungen vor?
- Wird ein Sprachmodell in der Datenbearbeitung verwendet?
- Erhält der Nutzer adäquate Informationen über den Einsatz von Chatbots?
- Auf welcher Grundlage erfolgt der Einsatz des AI-Systems?
- Sind angemessene Datensicherheitsvorkehrungen eingerichtet?
- Ist die Vornahme einer Datenschutz-Folgeabschätzung nötig? Wenn ja, wird sie durchgeführt?
- Erfolgt die Erfüllung der Informationspflichten sachgerecht?
- Können die Auskunfts- und Widerspruchsrechte der Betroffenen eingehalten werden?

Die Umsetzung der Aufgaben aus einer solchen Checkliste hat auch Auswirkungen auf die Ausgestaltung der vertraglichen Beziehungen, insbesondere wenn das die AI-Systeme einsetzende Unternehmen aus Vertraulichkeitsgründen spezifische Geheimhaltungspflichten eingegangen ist.

## 4. Datensicherheit und Datenschutz-Folgenabschätzung

Die Bedeutung der Datensicherheit hat erheblich

zugenommen, d. h. die Anforderungen an die Datenbearbeiter sind wesentlich gestiegen. AI-Systeme verursachen zweifellos Risiken, aber sie können auch zu einer Erhöhung des Datenschutzniveaus beitragen (z. B. Detektion unerwünschter Inhalte, Analyse von Programmcodes). Unternehmen müssen angemessene technische und organisatorische Massnahmen treffen, um die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit der Datenbearbeitung sicherzustellen.

Falls der Einsatz von AI-Systemen wegen der Verwendung neuer Technologien oder wegen der Art, dem Umfang, der Umstände und der Zweckerreichung von Datenbearbeitungen voraussichtlich hohe Risiken für die betroffenen Personen verursachen kann, ist der Verantwortliche überdies verpflichtet, eine Datenschutz-Folgenabschätzung mit Leitlinien zur Risikobewertung vorzunehmen.

Sinnvoll sind zudem interne Compliance-Audits als wirksames Instrument zur möglichen Aufdeckung von Compliance-Mängeln. Solche Audits bedürfen – gerade in Zeiten des starken technologischen Wandels – der periodischen Überprüfung mit Bezug auf ihre Wirksamkeit und Sachgemässheit. Die massgebenden Vorkehrungen entsprechen weitgehend den Anforderungen an das durch eine Due-Diligence-Orientierung geprägte Verhalten von Geschäftsleitungsmitgliedern eines Unternehmens.



bratschi

Agon Partners • Brandreport

# KI & Recht: Effizienz und bis zu 90 Prozent Einsparung

Die Digitalisierung revolutioniert die Rechtsbranche. Agon Partners nutzen KI, um zeitaufwendige Prozesse zu automatisieren und Unternehmen Kosteneinsparungen ermöglichen.



Patrick Krauskopf  
Anwalt in Zürich & New York,  
Verwaltungsratspräsident, Agon Partners



Tobias Gurtner  
CEO, Agon Partners Innovation AG

und potenzielle Risiken in Echtzeit erkennen, die für Menschen nicht zu erfassen sind. Beschaffungsstellen bei Bund, Kantonen, Gemeinden und Organisationen wie zum Beispiel dem Tiefbauamt des Kantons Graubünden profitieren von einer signifikanten Reduzierung der Kosten für manuelle Audits und Untersuchungen, während gleichzeitig die Compliance gestärkt wird.

## KI-Due-Diligence

KI spielt eine wichtige Rolle bei der Due Diligence in M&A-Deals. Agon Innovation nutzt KI-Software, die Verträge, Berichte und Dokumente automatisch prüft, Risiken identifiziert und Analysen in kürzester Zeit durchführt – effizienter und schneller als herkömmliche Methoden. «Die KI von Agon hat die Vertragsprüfung auf wenige Stunden reduziert und mir die Risiken auf verständliche Weise erläutert. Das war in einer zeitkritischen Phase ein echter Gewinn für unseren Verkaufsprozess», sagt Sandro Jörg, CEO Elite Autocenter.

## KI zur Datenanalyse

Interne Untersuchungen sind oft zeitaufwendig und ressourcenintensiv, da eine Vielzahl an Daten geprüft und analysiert werden muss. Agon Partners setzt eine KI-basierte Software ein, welche grosse Mengen an E-Mails, Chatverläufen und anderen digitalen Dokumenten durchsucht und analysiert, um relevante Beweise oder Auffälligkeiten zu finden. Durch den Einsatz von Natural Language Processing (NLP) und Machine Learning kann die Plattform Muster erkennen, die auf Unregelmässigkeiten hinweisen könnten, und so den Ermittlungsprozess erheblich beschleunigen.

## KI-Vertragsprüfung

Vertragsprüfungen binden oft Rechtsdienste und Anwälte. Die KI von Agon Partners analysiert Verträge automatisch, vergleicht Bedingungen mit Branchenstandards und erkennt mögliche Ungleichgewichte. Gerade bei komplexen Verträgen ist die automatisierte Prüfung ein wertvolles Werkzeug

Die fortschreitende Digitalisierung verändert die Rechtsbranche grundlegend. Künstliche Intelligenz (KI) spielt dabei eine immer grössere Rolle, indem sie zeitintensive und komplexe Prozesse automatisiert und so nicht nur die Effizienz steigert, sondern auch erhebliche Kosteneinsparungen ermöglicht. Agon Partners setzen KI-basierte Lösungen in der Rechtsanwendung um, die Kosteneinsparungen bei Unternehmen von bis zu 90 Prozent ermöglichen.

## KI-Kartell-Analyse

Die KI-gestützte Software von Agon Partners analysiert bei Beschaffungsvorhaben alle verfügbaren Daten, um mögliche kartellrechtliche Verstösse frühzeitig zu identifizieren. Durch den Einsatz von Machine Learning und fortschrittlicher Mustererkennung kann die Software ungewöhnliche Verhaltensmuster

«  
**Interne Untersuchungen sind oft zeitaufwendig und ressourcenintensiv, da eine Vielzahl an Daten geprüft und analysiert werden muss.**

zur Sicherstellung von Fairness und Gesetzeskonformität sicherzustellen, rechtliche Risiken zu reduzieren sowie Zeit und Kosten zu sparen.

## Ihre KI-Rechtsslösung

Kein Projekt ist zu komplex für uns. Von der ersten Analyse bis hin zur erfolgreichen Umsetzung begleiten wir Sie Schritt für Schritt mit lokalem Datenhosting und massgeschneiderten Lösungen, die darauf abzielen, Ihre Effizienz zu maximieren und gleichzeitig Ihre Kosten zu senken. Vertrauen Sie auf unsere Expertise als Ihr verlässlicher Partner für innovative KI-Lösungen in der Rechtsanwendung. Ihre Daten sind bei uns sicher. Dank Hosting in der Schweiz bleiben Ihre Informationen stets vertraulich und unter

striktem Schutz. Egal, ob es um die Vertragsprüfung, Due Diligence oder interne Untersuchungen geht – unsere hoch entwickelten Tools und Technologien passen sich nahtlos an Ihre individuellen Anforderungen an und sorgen dafür, dass Sie Ihre Ziele schneller und präziser erreichen. Mit uns an Ihrer Seite setzen Sie auf Innovation und Effizienzsteigerung, die genau auf Ihre Bedürfnisse zugeschnitten ist. Lassen Sie uns gemeinsam die Zukunft der Rechtsanwendung gestalten – sicher, zuverlässig und mit dem höchsten Mass an Datenschutz.

**Zu den Autoren**  
Tobias Gurtner, CEO  
Agon Partners Innovation AG

Patrick Krauskopf, Anwalt in Zürich und New York  
Verwaltungsratspräsident Agon Partners

+41 (0) 43 344 95 82  
info@agon-partners.ch  
agon-partners.ch



AGON PARTNERS