www.jusletter-it.eu

Rolf H. Weber

Künstliche Intelligenz und Datenschutz

In den letzten Jahren haben verfeinerte Gesetze in den meisten Ländern die persönlichkeitsbezogenen Grundprinzipien des Datenschutzes zu stärken versucht. Die neuesten technologischen Entwicklungen, v.a. die «Künstliche Intelligenz», führen nun aber zu weiteren (zusätzlichen) Herausforderungen. Das vorhandene Regelungsumfeld, sachgerecht ausgelegt und zur Anwendung gebracht, vermag indessen die meisten durch KI-Systeme hervorgerufenen Datenschutzprobleme zu bewältigen.

Beitragsart: Beiträge

Zitiervorschlag: Rolf H. Weber, Künstliche Intelligenz und Datenschutz, in: Jusletter IT 4. Juli 2024

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

EDITIONS WEBLAW

Inhaltsübersicht

1. Einleitung

[1] Der weite Begriff «Künstliche Intelligenz» (KI), der z.B. Erscheinungen wie automatisierte Entscheidungsabläufe, algorithmische Programmierungen und auch juristische Sprachmodelle bzw. allgemein Large Language Models (LLM) umfasst, hat in den letzten Monaten erheblich an Bedeutung gewonnen. Nachfolgend wird ein umfassendes Begriffsverständnis der KI in Betracht gezogen, welches nicht nur die generative KI, sondern auch das Machine Learning und das Deep Learning mitumfasst. Die KI vermag grosse Mengen an Daten zu verarbeiten und daraus Muster und Zusammenhänge zu eruieren, die für menschliche Analysen nicht leicht erkennbar sind. Solche Fähigkeiten hat die KI zu einem wertvollen Werkzeug in einer Vielzahl von Bereichen gemacht, aber auch neue und komplexe Fragen in Bezug auf den Datenschutz aufgeworfen.

[2] Entgegen verbreiteter Meinungsäusserungen ist die KI aber nicht nur eine Herausforderung für die Einhaltung der Datenschutzvorgaben, sondern algorithmische Programme können durchaus zur Verbesserung der Datensicherheit beitragen.[1] Beispiele sind (i) die Unterstützung bei der Detektion unerwünschter Inhalts, (ii) die Unterstützung bei der Berichterstattung zu Sicherheitsvorfällen, (iii) die Unterstützung bei der Erstellung und Analyse von Programmcodes (Untersuchungen mit Blick auf Sicherheitslücken) sowie (iv) die Unterstützung bei der Analyse des Datenverkehrs.[2] Datenschutz und KI stehen indessen in einem komplexen Wechselspiel zueinander; datenschutzrechtliche Vorgaben zur Anonymisierung von Daten oder der Grundsatz der Datensparsamkeit können etwa dazu beitragen, dass bestimmte KI-Techniken (z.B. Deep Learning), die

1 Rolf H. Weber, Juristische Sprachmodelle zwischen Transparenz und Datensicherheit, in: Erich Schweighofer et al. (Hrsg.), Sprachmodelle: Juristische Papageien oder mehr?, Bern 2024, S.19, S.22.

2 Eine konzise und übersichtliche Darstellung möglicher technischer Datenschutzmassnahmen findet sich bei David Rosenthal/Verein Unternehmens-Datenschutz, Datenschutz-Folgeabschätzung, Dezember 2023, Ziff. 3.12-3.22, https://www.rosenthal.ch/downloads/vud_dsfa.xlsm.

eine Bearbeitung grosser Mengen persönlicher Daten bezwecken, nur sehr eingeschränkt Verwendung finden dürfen.[3]

[3] Das Datenschutzrecht spielt in mehreren Phasen des KI-Einsatzes eine Rolle, nämlich (i) bei der Datenbeschaffung für den Aufbau eines KI-Systems, (ii) bei dessen Training, (iii) bei dessen Besitz und Betrieb sowie (iv) bei der praktischen Verwendung durch den Nutzer (Eingabe eines «Prompt»).[4] Die «Bedrohung» des Datenschutzes durch den Einsatz von KI ist in den letzten Monaten bereits Gegenstand verschiedener wissenschaftlicher Untersuchungen und praktischer Handlungsempfehlungen gewesen;[5] dass die Datenschutzregeln auf KI-Systeme grundsätzlich, wie der EDÖB zutreffend bemerkt,[6] anwendbar sind, dürfte unbestritten sein. Angesichts der vorhandenen Literatur rechtfertigt es sich, den vorliegenden Beitrag auf spezifische Themen zu konzentrieren und nicht alle Problembereiche anzusprechen;[7] die nachfolgenden Ausführungen beziehen sich demgemäss auf im Vordergrund stehende Herausforderungen, nämlich die DSG-Anknüpfungspunkte, die spezifischen Spannungsfelder zwischen KI und Datenschutz sowie einzelne Sonderfragen.

[4] Der Datenverkehr läuft angesichts des nicht-physischen Charakters von Daten sehr oft grenzüberschreitend ab. Aus diesem Grunde lehnt sich das Schweizer Datenschutzgesetz (DSG) über weite Strecken an die Datenschutz-Grundverordnung der EU (DSGVO) von 2016 an; die Äquivalenz der Normenwerke ist denn auch anerkannt.[8] Ungeachtet dieser Ausgangslage wird nachfolgend aber lediglich das DSG erörtert, und zwar deshalb, weil sich vom Regelungsansatz her betrachtet das DSG und die DSGVO grundlegend unterscheiden, denn das DSG beruht auf dem Prinzip der Zulässigkeit der Datenbearbeitung mit Verbotsvorbehalt, die DSGVO hingegen auf dem Prinzip des Verbots mit Erlaubnisvorbehalt.[9] Zwar löst sich dieser prinzipielle Unterschied in vielen praktischen Aspekten auf, doch gerade beim Einsatz von KI ergeben sich nicht selten unterschiedliche Rechtseinschätzungen, was die Konzentration dieses Aufsatzes auf das DSG legitimiert.[10]

---

3 Weber (Fn. 1), S. 23.

4 David Rosenthal, Datenschutz beim Einsatz generativer künstlicher Intelligenz, in: Jusletter 6. November 2023, Rz. 2 und Rz. 7.

5 Aus der neueren Literatur vgl. Florent Thouvenin/Stephanie Volz, «Datenschutz», White Paper, Juni 2024, https://www.itsl.uzh.ch/de/Wissenstransfer/Publikationen.html#Positionspapiere; Rosenthal (Fn. 4); Daniel W. Seiler/Marcel Griesinger, Spannungsfeld Künstliche Intelligenz (KI) und Datenschutzrecht, in: Jusletter 25. September 2023.

6 EDÖB, Geltendes Datenschutzgesetz ist auf KI direkt anwendbar, Version 11. Dezember 2023, https://www.edoeb.admin.ch/content/edoeb/de/home/kurzmeldungen/2023/20231109_ki_dsg.html.

7 Umfassende Überblicke bei Rosenthal (Fn. 4) und Seiler/Griesinger (Fn. 5); diese beiden Aufsätze enthalten auch viele weitere Literaturnachweise, die nachfolgend grundsätzlich nicht wiederholt werden. Thematisch nicht angesprochen werden hernach die besonders schützenswerten Personendaten, das Profiling, der grenzüberschreitende Datenverkehr, die Auftragsdatenbearbeitung, die Daten-Portabilität und die Datenschutz-Folgeabschätzung.

8 Art. 45 DSGVO; Entscheid vom 15. Januar 2024, Medienmitteilung des Bundesamtes für Justiz, https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-99695.html.

9 Vgl. Art. 6 i.V.m. Art. 31 DSG; dazu auch Seiler/Griesinger (Fn. 5) Rz. 10 mit Fn. 22.

10 Relevante Unterschiede betreffen insbesondere die Rechtfertigungsgründe und die automatisierten Einzelentscheidungen.

2. DSG-Anknüpfungspunkte

[5] Die beiden grundsätzlichen Regelungsziele des DSG sind der Schutz von Personendaten und die Gewährleistung der Datensicherheit. Das Ziel der Regulierungen besteht darin, normative Vorgaben auf der Basis des Grundsatzes der Technologieneutralität zu realisieren.[11]

2.1. Schutz von Personendaten

[6] Der Begriff der Personendaten ist im DSG sehr weit gefasst; nicht nur identifizierte Personen, sondern ebenso bestimmbare Personen geniessen den Schutz des DSG. Der Begriff der Bearbeitung umfasst jeden Umgang mit Personendaten (z.B. das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Offenlegen, Archivieren, Löschen und Vernichten der Daten, Art. 5 lit. d DSG). Ausserhalb des Anwendungsbereichs des DSG liegen deshalb nur die Sachdaten und die anonymisierten bzw. pseudonymisierten Daten[12] sowie die Datenbearbeitung zu nicht-personenbezogenen Zwecken.[13]

[7] Im Kontext der KI ist zu differenzieren zwischen den Personendaten als «Input» und den Personendaten als «Output»; die Differenzierung ist relevant, weil diejenigen Personen, welche die DSG-Vorschriften beachten müssen (Verantwortlicher oder Auftragsbearbeiter), nicht identisch sind.[14] Im Lichte der vorerwähnten Phasen des KI-Einsatzes fallen der Aufbau eines KI-Systems, dessen Training und dessen Besitz/Betrieb in den «Input»-Bereich, während die möglichen Verwendungen zum «Output»-Bereich gehören.[15]

[8] Mit «*Input*» ist konkret gemeint, dass die Eingaben zur Verwendung eines KI-Systems keine geschützten Personendaten enthalten dürfen, sofern nicht sichergestellt ist, dass der Anbieter des KI-Systems sich bei der weiteren Arbeit mit dem KI-System an die Datenschutzvorgaben hält. Personendaten können in den von den Benutzern eingegebenen «Prompts» enthalten sein, aber sich auch aus dem Sammeln von Daten aus öffentlichen Quellen (durch ein sog. «Crawlen») ergeben.[16] Seitens des KI-Anbieters dürfen die allenfalls übermittelten Personendaten wegen des Grundsatzes der Zweckbindung insbesondere nicht für andere Zwecke verwendet werden (z.B. das Training eigener Modelle)[17] und es sind technische Vorsichtsmassnahmen geboten, wenn ein Outsourcing der Datenbearbeitung erfolgt oder wenn sich der Auftragsbearbeiter im Ausland befindet.

[9] Datenschutzrechtliche Problembereiche, welche die durch KI-Systeme verfügbar gemachten «*Outputs*» betreffen, sofern Personendaten enthalten sind, bestehen insbesondere mit Blick auf drei Erscheinungen:[18] (i) KI-Systeme können «halluzinieren», d.h. Inhalte erfinden, die dem Be-

11 Thouvenin/Volz (Fn. 5), S. 3.

12 Eingehender zur Verschlüsselung von Trainingsdaten Dany Pina, Die Offenbarung von KI-Patenten, Zürich 2024, S. 46 ff. m.w.H.

13 Zu diesem im KI-Kontext wichtigen Bereich vgl. nachfolgend Rz. 19 ff.

14 Zu den verschiedenen «Input»- und «Output»-Faktoren eingehend Rosenthal (Fn. 4), Rz. 46 ff.; zur unterschiedlichen Verantwortlichkeit für diese Faktoren vgl. Ders., Rz. 18.

15 Im Einzelnen zu den Elementen eines KI-Modells vgl. David Rosenthal, Was in einem KI-Modell steckt und wie es funktioniert, Blog Vischer, Teil 17, Mai 2024, https://www.vischer.com/kuenstliche-intelligenz/.

16 Seiler/Griesinger (Fn. 5), Rz. 8 und Rz. 31.

17 Zum Sonderproblem des Fine-Tuning eines KI-Systems vgl. Rosenthal (Fn. 4), Rz. 44 f.

18 Rosenthal (Fn. 4), Rz. 50 ff.

nutzer als wahre Informationen erscheinen. (ii) Outputs von KI enthalten ggf. ungewollt Personendaten. (iii) Der Output der KI verzerrt allenfalls die Daten, d.h. es entsteht ein «Bias», der mit Blick auf die datenschutzrechtlichen Grundsätze der Richtigkeit, Verhältnismässigkeit sowie von Treu und Glauben zu Problemen führt. In allen drei Situationen sind die datenschutzrechtlichen Herausforderungen anhand der konkreten Gegebenheiten zu analysieren.

2.2. Datensicherheit

[10] Ein wichtiger Aspekt des Datenschutzrechts ist die Datensicherheit (Art. 8 DSG). Wie erwähnt[19] dürfen beim Stichwort «Datensicherheit» nicht nur mögliche Risiken der KI in Betracht gezogen werden, sondern die Verwendung von KI-Systemen vermag auch zu einer Erhöhung der Datensicherheit beizutragen, weil solche Systeme strukturierte Programmabläufe ermöglichen.

[11] Als Risiken von KI-Programmen und algorithmischen Verfahren lassen sich die fehlende Vertraulichkeit der eingegebenen Daten, die mangelnde Faktizität und Reproduzierbarkeit, die ungenügende Aktualität, die fehlerhafte Reaktion auf spezifische Eingaben und die Anfälligkeit für «versteckte» Dateninfiltrationen mit manipulativer Absicht identifizieren. Konkrete Risikosituationen betreffen (i) das Social Engineering (z.B. durch Preisgabe von Daten, Umgehung von Schutzmassnahmen, Installierung eines Schadcodes), (ii) den Einsatz von Malware (z.B. Erzeugung eines Schadcode ohne viel Hintergrundwissen dank ausgereifterer Code-Generierungsfähigkeiten, selbst bei Vorhandensein polymorpher Schadsoftware) und (iii) das Auftreten einer sog. «Hoax» (z.B. Falschmeldung wegen Desinformation oder Propaganda).[20]

[12] Die Datensicherheit ist mindestens so sehr eine technische wie eine rechtliche Herausforderung; aus diesem Grunde konzentrieren sich die nachfolgenden Ausführungen auf den vorgenannten Schutz von Personendaten.

3. Spannungsfelder zwischen künstlicher Intelligenz und Datenschutz

[13] Die Zahl der Spannungsfelder zwischen KI und Datenschutz ist gross; neben einer kurzen Erläuterung von einzelnen weniger zentralen Themenfeldern und Sonderfragen kommen schwergewichtig die Datenbearbeitungsgrundsätze, die Rechtfertigungsgründe, die automatisierten Einzelentscheidungen und die Verwendung von «Output»-Daten zur Sprache.

3.1. Datenbearbeitungsgrundsätze

[14] Das DSG geht (wie erwähnt im Gegensatz zur DSGVO) vom Grundsatz aus, dass eine Datenbearbeitung zulässig ist, wenn der Verantwortliche die gesetzlich statuierten Datenbearbeitungsprinzipien einhält, es gilt also kein Erlaubnisvorbehalt. Die Beschaffung und Bearbeitung von Personendaten setzen im Kontext der Entwicklung, des Trainings, der Validierung und des

19 Vgl. vorne Rz. 2.

20 Weber (Fn. 1), S. 24.

Testens von KI-Systemen aber insbesondere die Beachtung der folgenden Datenschutzprinzipien voraus:[21]

- *Grundsatz der Erkennbarkeit*: Oft ist die Beschaffung und Bearbeitung von Personendaten für die Betroffenen nicht erkennbar, weil die Daten vom KI-System aus verschiedenen Quellen bezogen werden, ohne dass die betroffenen Personen eine Information erhalten.
- *Grundsatz der Zweckbindung*: KI-Systeme bearbeiten Daten oft zu einem anderen Zweck als demjenigen, der bei der ursprünglichen Beschaffung relevant gewesen ist, insbesondere im Falle eines «General Purpose AI-Systems».[22]
- *Grundsatz der Datenminimierung*: Die Verwendung von mehr Daten durch KI-Systeme verbessert meist die Ergebnisse, d.h. den «Output», was aber dem Ziel der Datenminimierung widerspricht.
- *Grundsatz der Speicherbegrenzung*: Zwar werden die verwendeten Personendaten regelmässig nicht im trainierten KI-System gespeichert, doch entsteht ein DSG-Problem, sofern nach Abschluss der Entwicklung eine Speicherung in einer gesonderten Datenbank erfolgt.

[15] Ein weiterer zentraler Grundsatz der Datenbearbeitung ist die Datenrichtigkeit; der Verantwortliche muss sich vergewissern, dass die gesammelten Daten während der ganzen Aufbewahrungsdauer ihre Richtigkeit behalten.[23] In Frage steht also die inhaltliche Korrektheit der Daten und die Vermeidung von Fehlinformationen, was bei grossen KI-Systemen die Einrichtung umfangreicher technischer Sicherheitsvorkehren notwendig macht.

[16] Der Einsatz von KI führt nicht in jeder Situation zu einer ungenügenden Beachtung der Datenbearbeitungsgrundsätze, vielmehr sind Einzelfall-Analysen durchzuführen; für gewisse Zwecke von KI-Trainings mag die Verwendung möglichst vieler Informationen ungeachtet des Datenminimierungsgebots sinnvoll sein, um dem Grundsatz der Datenrichtigkeit Genüge zu tun.

[17] Überdies lässt sich die Datenbearbeitung durch Rechtfertigungsgründe legitimieren, die hernach im Einzelnen zu beurteilen sind.

3.2. Rechtfertigungsgründe

[18] Weil das DSG vom Grundsatz der Zulässigkeit der Bearbeitung von Personendaten im Falle der Einhaltung der Datenbearbeitungsprinzipien ausgeht bzw. im Falle der Nichteinhaltung den Nachweis einer Rechtfertigung der Datenbearbeitung einschränkt, haben die Rechtfertigungsgründe (Art. 31 DSG) eine grosse praktische Bedeutung. Nachfolgend wird der für KI-Systeme zentrale Aspekt der Datenbearbeitung zu nicht-personenbezogenen Zwecken gesondert, vor den allgemeinen Rechtfertigungsgründen, erläutert.[24]

---

21 Allgemein zu den Datenbearbeitungsgrundsätzen Reto Fanger, OFK-DSG, Kommentar, Zürich 2023, Art. 6 Rz. 4 ff.; zu den KI-spezifischen Themenstellungen vgl. Thouvenin/Volz (Fn. 5), S. 4; Seiler/Griesinger (Fn. 5), Rz. 10.

22 Insoweit stellt sich das besondere Problem der Zweitnutzung bzw. der Zweitverwertung; vgl. dazu Rosenthal (Fn. 4), Rz. 28, mit weiteren Ausführungen.

23 Allgemein dazu vgl. Fanger (Fn. 21), Rz. 11 m.w.H.; zu den KI-spezifischen Themenstellungen vgl. Paulina J. Pesch/Rainer Böhme, Verarbeitung personenbezogener Daten und Datenrichtigkeit bei grossen Sprachmodellen, MMR 12/2023, S. 917 ff. m.w.H.

24 Rosenthal (Fn. 4), Rz. 34 ff. erläutert diesen Rechtfertigungsgrund unter dem Titel «knifflige Fragen».

3.2.1. Datenbearbeitung zu nicht-personenbezogenen Zwecken

[19] Zu den überwiegenden Interessen des Verantwortlichen für eine Datenbearbeitung gehört der Rechtfertigungsgrund der Bearbeitung zu nicht-bezogenen Zwecken (Art. 31 Abs. 2 lit. e DSG);[25] im Vordergrund stehen dabei Forschung, Planung oder Statistik. KI-Systeme zielen in der Praxis oft darauf ab, nicht Erkenntnisse mit Bezug auf spezifische Personen zu gewinnen, sondern Programme zu entwickeln, welche bestimmte Aufgaben möglichst gut zu erfüllen in der Lage sind. Eine solche Bearbeitung ist nicht vornehmlich personenbezogen.

[20] Immerhin setzt dieser Rechtfertigungsgrund auch die Erfüllung weiterer Voraussetzungen voraus:[26] (i) Sobald der Bearbeitungszweck es erlaubt, sind die Daten zu anonymisieren; technische Massnahmen ermöglichen in der Praxis oft eine solche Anonymisierung von KI-Systemen. (ii) Im Falle der Bearbeitung von besonders schützenswerten Personendaten darf eine Bekanntgabe an Dritte nur so erfolgen, dass die betroffene Person nicht bestimmbar ist; meist lässt sich diese Voraussetzung wohl erfüllen. (iii) Die Veröffentlichung von Ergebnissen muss in einer Art erfolgen, dass die betroffenen Personen nicht bestimmbar sind. Ob diese Anforderung bei KI-Systemen erfüllt ist, hängt von der konkreten «Veröffentlichung» der entsprechenden Daten ab.

[21] Im Einzelnen ergeben sich aber schwierige Abgrenzungsfragen bei der Beurteilung der Datenbearbeitung zu «nicht-personenbezogenen Zwecken» oder auch beim «überwiegenden Interesse» an der Datenbearbeitung gemäss Art. 31 Abs. 2 DSG; zutreffend nimmt die Lehre in neuester Zeit diese Rechtfertigungsgründe etwas genauer unter die Lupe.[27]

[22] Weil der Auslegungsspielraum für die Gerichte relativ gross ist, stellt sich die Frage, ob der Gesetzgeber die gegebene Liste für das Vorliegen eines überwiegenden Interesses (Art. 31 Abs. 2 DSG) um ein weiteres Beispiel (Datenbearbeitung für das Trainieren, Validieren und Testen von KI-Systemen) ergänzen oder ob der EDÖB in einem Leitfaden bzw. Merkblatt klarstellen sollte, dass die Inbetriebnahme eines KI-Systems nicht als Veröffentlichung von Ergebnissen gilt.[28] Einzelne Stimmen gehen demgegenüber von einer normativen Kraft des Faktischen bzw. einer «sozialen Realität» aus, die wohl darauf hinauslaufe, dass gewisse «Datenschutz-Beeinträchtigungen» durch KI-Systeme von der Gesellschaft mit der Zeit hingenommen würden.[29]

3.2.2. Weitere Rechtfertigungsgründe

[23] (i) Der aus der Sicht des Gesetzgebers naheliegendste Grund für eine Rechtfertigung der Datenbearbeitung ist die Einwilligung der betroffenen Person. Im KI-Kontext hat dieser Grund indessen praktisch nur eine geringe Bedeutung: Die Einholung der Einwilligung des Betroffenen ist beim «Input» von Daten in KI-Systeme sehr schwierig und mit hohen Hürden verbunden;[30] deshalb ist es wenig erstaunlich, dass eine Umfrage des Vereins Unternehmens-Datenschutz bei

25 Eingehender dazu Thouvenin/Volz (Fn. 5), S. 4 f. und Rosenthal (Fn. 4), Rz. 35 ff., insbesondere Rz. 38.

26 Vgl. auch Thouvenin/Volz (Fn. 5), S. 4 f.

27 Vgl. Thouvenin/Volz (Fn. 5), S. 5; Rosenthal (Fn. 4), Rz. 36.

28 Thouvenin/Volz (Fn. 5), S. 5.

29 Im Einzelnen Rosenthal (Fn. 4), Rz. 40–42; die Einwände gegen diese Betrachtungsweise entsprechen den Überlegungen zur sog. normativen Kraft des Faktischen.

30 Vgl. Seiler/Griesinger (Fn. 5), Rz. 14 (wenn zwar in problematischer Weise relativierend Dies., Rz. 26).

seinen Mitgliedern im Jahre 2023 zum Ergebnis kam, die Einwilligung stelle bei den meisten Unternehmen nur in 10%-20% der Fälle einen Rechtfertigungsgrund dar.[31]

[24] Zudem führen selbstlernende Algorithmen über die Zeit zu Veränderungen in der Datenbearbeitung, die zu Beginn ggf. nicht vorausgesehen werden konnten; dementsprechend deckt sogar eine erfolgte Einwilligung neue, ursprünglich nicht bekannte Vorgänge in KI-Systemen nicht ab. Weil es somit an der Einwilligung im Rahmen von KI-Systemen regelmässig fehlt, haben andere Rechtfertigungsgründe eine grössere praktische Bedeutung.[32]

[25] (ii) Die Berufung auf ein berechtigtes Interesse des Verantwortlichen ist – ausser in bestimmten Konstellationen mit besonders schützenswerten Personendaten – dann in Betracht zu ziehen, wenn das KI-System höherwertigen Zielen dient. Das Spannungsfeld zwischen DSG- und KI-Interessen, das sich nicht gestützt auf allgemeine Überlegungen, sondern vielmehr nur mit Blick auf die konkreten Umstände auflösen lässt, hat im Artificial Intelligence Act (AIA) der EU eine besondere Regelung erfahren: So findet sich in Art. 10 Ziff. 5 AIA eine Anordnung zur Bearbeitung von besonderen Personendaten-Kategorien für das Entdecken und Korrigieren von Verzerrungen («Biases»): Anbieter von KI-System sind insbesondere verpflichtet, angemessene Garantien für die Grundrechte und die Grundfreiheiten der Betroffenen einzurichten.[33]

[26] (iii) Überdies ist in diesem Kontext auch das Spannungsfeld zwischen der öffentlichen Information und dem Datenschutz zu beachten (Art. 31 Abs. 2 lit. f DSG). KI-Systeme sammeln nicht nur Personendaten, sondern durch ein oft umfassendes «Crawlen» auch sog. öffentliche Informationen. Datenschutzrechtlich scheint das «Crawlen» auf den ersten Blick nicht problematisch zu sein, denn grundsätzlich verfügen Informationen aus öffentlich verfügbaren Quellen nicht über einen besonderen Schutz. Dennoch ist nicht zu übersehen, dass nach Auffassung des EDÖB auch veröffentlichte Personendaten weiterhin vom Datenschutz erfasst sind und nicht frei verwendet werden dürfen.[34]

[27] Die Spezialregelung von Art. 30 Abs. 3 DSG privilegiert den Verwender öffentlicher Inhalte lediglich unter dem Vorbehalt, dass der Inhalt mit Zustimmung der betroffenen Person allgemein zugänglich gemacht und der Nutzung im Einzelfall nicht widersprochen worden ist.[35] Das Öffentlichkeitsinteresse an KI-Systemen allgemein ist überdies ein Thema des nachfolgend detaillierter zu erörternden Transparenzprinzips.[36]

[28] In neuester Zeit stellen grosse KI-Anbieter zudem in Aussicht, in ihren (versteckten) Datenschutzbestimmungen eine Einwilligung der Vertragspartner vorzusehen, die besagt, dass auch «Informationen, die über die Produkte und Dienstleistungen von Meta geteilt werden», für die

31 Vgl. Verein Unternehmens-Datenschutz, Benchmarking 2023: Informationelle Selbstbestimmung, https://www.vud.ch/customer/files/180/VUD_Benchmarking-2023_Informationelle-Selbstbestimmung.pdf.

32 Vgl. dazu auch Thouvenin/Volz (Fn. 5), S. 5; Seiler/Griesinger (Fn. 5), Rz. 16 ff.

33 Dazu International Association of Privacy Professionals (IAPP), The AI Act's debiasing exception to the GDPR, 21 February 2024, https://iapp.org/news/a/the-ai-acts-debiasing-exception-to-the-gdpr; zur Diskriminierungsproblematik vgl. allgemein Florent Thouvenin/Stephanie Volz/Soraya Weiner/Christoph Heitz, Diskriminierung beim Einsatz Künstlicher Intelligenz (KI): Technische Grundlagen für Rechtsanwendung und Rechtsentwicklung, Rz. 4 ff., in diesem Jusletter.

34 Vgl. EDÖB in Zusammenarbeit mit ausländischen Datenschutzbehörden: Gemeinsame Erklärung «Data Scraping» und Datenschutz, 24. August 2023, https://datenrecht.ch/edoeb-et-al-gemeinsame-erklaerung-zu-data-scraping-und-datenschutz/; vgl. auch Seiler/Griesinger (Fn. 5), Rz. 19.

35 Rosenthal (Fn. 4), Rz. 30; vgl. auch Ders., Rz. 32 f.

36 Vgl. hinten Rz. 43 ff.

Bearbeitung in KI-Systemen herangezogen werden können;[37] erfasst sind damit Daten, Fotos usw., die von den Nutzern täglich auf den Plattformen hochgeladen werden; ob eine solche Einwilligung der Betroffenen den Klarheitsvorgaben des DSG Genüge tut, erscheint immerhin als sehr zweifelhaft und hat denn auch die EU-Datenschutzbehörden bereits auf den Plan gerufen.

3.3. Automatisierte Einzelentscheidungen

[29] Vorausschauend haben Art. 22 DSGVO und Art. 21 DSG schon vor einem breiten Einsatz von KI-Systemen eine Regelung zu den automatisierten Einzelentscheidungen eingeführt; inhaltlich geht der kurz zu erläuternde Art. 21 DSG weniger weit als der umfassendere Art. 22 DSGVO.[38] Bei der automatisierten Bearbeitung von Personendaten unterliegt der Verantwortliche einer Informationspflicht an die Betroffenen, falls die Bearbeitung eine rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.[39] Automatisierte Bearbeitungen kommen insbesondere in KI-Systemen vor, die auf maschinellem Lernen basieren und die in der Lage sind, komplexe Vorhersagen oder Entscheidungen ohne menschliches Zutun zu treffen.[40]

[30] Die betroffene Person hat das Recht, Widerspruch gegen eine automatisierte Einzelentscheidung einzulegen, ausser wenn diese Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist oder ein öffentlich-rechtlicher Rechtfertigungsgrund vorliegt.[41] Die Auslegung dieser Gründe kann nach den allgemeinen Grundsätzen erfolgen, weil sie nicht KI-spezifisch sind.

[31] Ein für KI-Systeme besonders relevantes Problem von Art. 21 DSG liegt darin, dass der Gesetzeswortlaut verlangt, es müsse sich um «ausschliesslich» automatisierte Datenbearbeitungen (ohne Dazutun einer natürlichen Person) handeln (Abs. 1). Dieser Tatbestand mag bei ADM-Systemen («algorithmic decision-making») und beim Profiling von Personen in der Regel vorliegen.[42] Im Kontext des Einsatzes grosser KI-Systeme findet aber nicht selten zusätzlich noch ein nicht automatisiertes Monitoring im Sinne einer Plausibilitätsüberprüfung statt, was an sich die Erfüllung des Kriteriums «ausschliesslich» in Frage stellt. Die Lehre geht davon aus, dass nicht das «Können» einer Beeinflussung der Entscheidung durch eine natürliche Person massgebend ist, sondern die Frage, «ob eine Überprüfung [...] durch eine natürliche Person tatsächlich erfolgt, welche zudem rechtlich und faktisch in der Lage wäre, den maschinell getroffenen Entscheid umzustossen».[43]

---

37 Vgl. Tages Anzeiger vom 13. Juni 2024, S. 17; zur Intervention der EU-Datenschutzbehörden vgl. NZZ vom 25. Juni 2024, S.22. Demgegenüber behauptet Apple in seinen öffentlichen Verlautbarungen, dem Datenschutz bzw. der Privatsphäre eine besondere Aufmerksamkeit zu schenken (vgl. NZZ vom 12. Juni 2024, S. 23).

38 Für einen detaillierten Überblick vgl. Fabienne Suter, Automatisierte Einzelentscheidungen im (Schweizer) Datenschutzrecht, Diss. Zürich 2024, S. 245 ff.

39 Vgl. dazu Adrian Bieri/Julian Powell, OFK-DSG, Kommentar, Zürich 2023, Art. 21 Rz. 7 f.

40 Seiler/Griesinger (Fn. 5), Rz. 56.

41 Rosenthal (Fn. 4), Rz. 6.

42 Vgl. Suter (Fn. 38), S. 294 ff.

43 Bieri/Powell (Fn. 39), Rz. 6.

3.4. Verwendung von Personendaten

[32] Wie erwähnt, ist bei KI-Systemen zwischen dem «Input» und dem «Output» zu differenzieren. Auch bei der Verwendung von Personendaten («Output») sind in vergleichbarer Weise die zuvor erläuterten Grundsätze der Datenbearbeitung zu beachten. Zusätzlich gewinnt aber der Grundsatz der Richtigkeit der Daten an Bedeutung;[44] gerade im Kontext von KI-Systemen ist von besonderer Bedeutung, dass sich die Richtigkeit mit Blick auf den Zweck der Datenbearbeitung beurteilt und dieser Zweck dem Risiko einer «Halluzination» (z.B. durch frei erfundene Angaben über Personen) unterliegt.[45] Werden «Prompts» (mit Personendaten) von KI-Nutzern eingegeben und hernach verarbeitet, hat der Betreiber von KI-Systemen beim «Output»-Angebot oft die Rolle eines Auftragsbearbeiters.[46]

[33] Gelingt es einem Dritten, durch gezielte Abfragen bzw. Attacken einzelne Personendaten von Betroffenen aus KI-Systemen zu entnehmen, die z.B. zu Trainingszwecken verwendet worden sind, liegt ggf. ein (unfreiwilliges) Bekanntgeben von Personendaten (Art. 5 lit. e DSG) vor. Das Bekanntgeben muss den Datenbearbeitungsgrundsätzen genügen; der Betreiber des KI-Systems unterliegt deshalb zudem dann einem Haftungsrisiko, wenn er den anwendbaren Datensicherheitsvorkehren nicht genügt.[47] Im Einzelnen können sich überlagernde Datenbearbeitungen aber schwierige Abgrenzungsprobleme hervorrufen: Der KI-Nutzer trägt die Verantwortung, wenn er die «Prompts» mit den Personendaten nicht sachgerecht gemäss den technischen Vorgaben des KI-Anbieters implementiert; der Betreiber des KI-Systems hat für die DSG-kompatible Bearbeitung der Personendaten einzustehen.[48]

3.5. Informations- und Sorgfaltspflichten

[34] Die Verantwortlichen haben die Pflicht, die betroffenen Personen über die Verarbeitung ihrer Daten zu informieren (Art. 19 ff. DSG). Diese über die erwähnte Aufklärung zu den automatisierten Einzelentscheidungen[49] hinausgehenden Informationspflichten stellen einen zentralen Pfeiler des Datenschutzrechts dar. Einerseits wird durch die Informationen die Transparenz der Datenbearbeitung erhöht und andererseits ermöglichen die Informationen den betroffenen Personen die Ausübung ihrer Auskunfts- und Korrektur- bzw. Widerrufsrechte.

[35] Der Anbieter von KI-Systemen hat demgemäss die KI-Nutzer darüber zu informieren, wie ihre Daten konkret bearbeitet werden, unter Hinweis auf die Zwecke der Bearbeitung und die verwendeten Algorithmen.[50] Im Falle der Beurteilung von Kreditrisiken ist der Nutzer eines KI-Systems zum Beispiel darüber zu informieren, welche Daten (z.B. Kreditverlauf, Einkommen, Alter) konkret Verwendung finden, wie die Datenbearbeitung erfolgt und wie das System seine Vorhersagen trifft. Die Verfügbarkeit der Information ist im Übrigen auch deshalb relevant,

44 Vgl. vorne Rz.15.

45 Thouvenin/Volz (Fn. 5), S. 7.

46 Eingehender dazu Rosenthal (Fn. 4), Rz. 16 f.

47 Vgl. vorne Rz. 19 ff.

48 Vgl. zur Sanktionierung von DSG-Verstössen auch David Rosenthal, Datenschutz und KI: Worauf in der Praxis zu achten ist, in: Jusletter IT 26. April 2022, Rz. 55.

49 Vgl. vorne Rz. 29 ff.

50 Seiler/Griesinger (Fn. 5), Rz. 52 ff., v.a. Rz. 53.

weil ggf. Auskunftsansprüche vom Betroffenen geltend gemacht werden, die zur Herausgabe von Informationen zwingen.[51]

[36] Die Informationspflichten verursachen aber grosse Herausforderungen im Kontext der KI-Systeme; Algorithmen sind oft komplex und für Nicht-Experten schwer zu verstehen.[52] Transparente Information bedeutet, dass gemäss den Prinzipien der Erklärbarkeit und Nachvollziehbarkeit den KI-Nutzern verständlich zu machen ist, wie und mit welchem Zweck die Datenbearbeitung abläuft.[53] Abgesehen von der in vielen Situationen vorliegenden Schwierigkeit, eine sachgerechte «Aufklärung» vorzunehmen, erweist sich auch eine Abwägung zwischen den Interessen der KI-Nutzer an der Kenntnis über die datenbezogenen Vorgänge und den Interessen der Anbieter von KI-Systemen an der Vertraulichkeit individueller Programmierungen, die auf dem Konzept des Unternehmensgeheimnisses basiert, als notwendig.[54]

[37] Überdies ermöglicht es die Technik, dass sich Algorithmen im Laufe der Zeit «selbstständig» anpassen bzw. verfeinern und damit das KI-System weiterentwickeln, was die Übermittlung von Informationen an die Nutzer des KI-Systems erschwert. In solchen Fällen wäre an sich eine repetitive Information sachgerecht; in welcher Art und Weise in dieser Konstellation die Information in klarer und nachvollziehbarer Weise bereitgestellt werden kann, um das Recht der Nutzer auf Information zu gewährleisten, stellt die Anbieter von KI-Systemen aber vor nicht zu unterschätzende Probleme und muss Anlass für eine verbesserte «Medienkompetenz» der Mitarbeitenden sein.[55]

3.6. Verantwortlichkeit

[38] Fehlt es an der Beachtung der Datenbearbeitungs- oder Datenverwendungsgrundsätze im Kontext eines KI-Systems, stellt sich die Frage, wer die Verantwortung für eine etwaige DSG-Verletzung zu übernehmen hat. Im Vordergrund steht der Ersteller bzw. Besitzer und damit typischerweise der Anbieter, nicht der Kunde des KI-Systems; datenschutzrechtlich liegt der Anknüpfungspunkt nämlich bei der Festlegung der wesentlichen Parameter (Zweck und Mittel) der Datenbearbeitung (Art. 5 lit. j DSG).[56]

[39] Die Haftungszuordnung ist deshalb mit Schwierigkeiten behaftet, weil oft nicht klar ist, wer in welchem Stadium ggf. Daten bearbeitet.[57] Auch der Auftragsbearbeiter kommt bei Datenbearbeitungen in der Cloud als verantwortliche Person in Betracht. Im Falle von reinen Hosting-Tätigkeiten vermag unter Umständen eine Haftungsbeschränkung gestützt auf die Grundsätze der Hosting-Provider-Haftung einzutreten.[58]

---

51 Vgl. hinten Rz. 48 f.

52 Vgl. dazu auch Seiler/Griesinger (Fn. 5), Rz. 54.

53 Eingehender dazu Weber (Fn. 1), S. 22.

54 Vgl. dazu Luc Desaunettes, Von den Zünften zur künstlichen Intelligenz: Die Renaissance von Geschäftsgeheimnissen, Max-Planck-Gesellschaft, München 2018, https://www.mpg.de/12529808/ip_jb_2018.

55 Zur Transparenz gegenüber den Betroffenen vgl. hinten Rz. 43 ff.; zur «Medienkompetenz» vgl. auch Rosenthal (Fn. 4), Rz. 56.

56 Rosenthal (Fn. 4), Rz. 20 und Rz. 22.

57 Zu den Haftungsfragen im Besonderen vgl. Isabelle Wildhaber, KI und Haftung: Lösungsansätze für die Schweiz, Rz. 20 ff., in diesem Jusletter IT.

58 Rosenthal (Fn. 4), Rz. 23

4. Sonderfragen

4.1. Trainings-KI

[40] Trainingsdaten lassen oft keinen direkten Schluss auf bestimmbare Personen zu; soweit es am Kriterium der Bestimmbarkeit fehlt, entfallen die datenschutzrechtlichen Herausforderungen. In der Regel erfolgt die Verschlüsselung der Personendaten im Laufe bzw. am Ende des Lernprozesses; in neuerer Zeit wird aber vermehrt diskutiert und technologisch versuchsweise umgesetzt, Lösungen für eine Verschlüsselung bereits vor dem Lernprozess zu implementieren.[59] In einem solchen Fall wäre der Personenbezug nicht nachvollziehbar, was die DSG-Relevanz beseitigen würde.

[41] Wird der Personenbezug von Trainingsdaten nicht ausgeschlossen, ergibt sich bei ihrem Einsatz das Problem, dass der finale Bearbeitungszweck oft vom ursprünglichen Datenbearbeitungszweck abweicht. In einer solchen Konstellation stellt sich die Frage, ob eine Zweitverwertung vorliegt; verschiedene Formen der Zweitverwertung von Daten haben eine immer grössere Bedeutung und rufen nach einer datenschutzrechtlichen Beurteilung.[60]

[42] Nach dem revidierten DSG (Art. 6 Abs. 3) muss der Zweck einer Zweitverwertung für die betroffene Person bereits bei der Beschaffung von Daten mindestens erkennbar sein; der «Sekundärzweck» (wie z.B. das Training der KI) ist deshalb dann vom Zweckbindungsgrundsatz gedeckt, wenn er mit dem ursprünglichen «Primärzweck» vereinbar und für den Betroffenen in der Entwicklung auch nachvollziehbar ist.[61]

4.2. Transparenz

[43] Ein grundlegendes Problem beim Einsatz von KI-Systemen besteht – wie erwähnt – in der mangelnden Transparenz mit Bezug auf deren Funktionsweise (z.B. Einsatz von Algorithmen, angewendete Methoden); akzentuiert wird das Risiko der Intransparenz bei den kaum steuerbaren selbstlernenden Algorithmen.[62] Die Transparenz ist denn auch im dichten Regulierungswerk des AIA der EU ein zentrales Thema.[63]

[44] Selbst soweit es datenschutzrechtlich gesetzliche Transparenzanforderungen gibt, wie z.B. mit Blick auf automatisierte Entscheidungen (Art. 21 DSG), ist deren Wirkung nicht zu überschätzen.[64] Empirische Untersuchungen zu den vorhandenen daten- und verbraucherschutzrechtlichen Informationspflichten lassen nämlich daran zweifeln, ob die gesetzlich geforderte Transparenz stets einen Mehrwert für die betroffenen Personen generiert und ihren angedachten Zweck erfüllt.[65] Die zur Verfügung gestellten Informationen sind oft nicht ausreichend ver-

59 Vgl. Pina (Fn. 12), S. 46 f.

60 Rosenthal (Fn. 4), Rz. 28.

61 Vgl. auch Thouvenin/Volz (Fn. 5), S. 4.

62 Weber (Fn. 1), S. 21.

63 Im Einzelnen dazu Daria Bohatchuk/Alfred Früh, Transparenz im Fokus der Europäischen KI-Verordnung, in: Jusletter 12 Februar 2024, Rz. 6 ff.

64 Vgl. vorne Rz. 36.

65 Dazu in Einzelnen Weber (Fn. 1), S. 21.

ständlich und überfordern angesichts der Informationsintensität (Länge, Detaillierungsgrad) die betroffenen Personen.[66]

[45] Weiter müssen KI-Systeme grundsätzlich erklärbar und interpretierbar sein, um den betroffenen Personen die Nachvollziehbarkeit von algorithmischen Vorgängen zu ermöglichen. Notwendig ist somit, abhängig vom Wissenshorizont des Betroffenen und der Bedeutung der Vorgänge, eine ausreichende Verständlichkeit, d.h. die zugrunde liegende Logik hat auch begreiflich zu sein, was bei komplexen technischen Vorgängen nur schwer zu erreichen ist.[67]

[46] Das DSG scheibt beim Einsatz von KI-Systemen im Rahmen der Bearbeitung von Personendaten nicht ausdrücklich eine Information der Betroffenen vor. Bearbeiten indessen KI-Anbieter die Daten von betroffenen Personen in einer Art und Weise, mit welcher nicht hat gerechnet werden müssen, und die sich in relevanter Weise negativ auswirken kann, macht der Grundsatz der Transparenz eine Information erforderlich, selbst wenn Art. 19 DSG nicht direkt als Rechtsgrundlage herangezogen werden kann.[68]

4.3. Betroffenenrechte

[47] Bei den Betroffenenrechte stehen die Auskunftsrechte sowie die Ansprüche auf Widerspruch und Korrektur im Vordergrund.

4.3.1. Auskunftsrecht

[48] Das Auskunftsrecht setzt voraus, dass der Betreiber eines KI-Systems tatsächlich Personendaten verarbeitet; die betroffene Person hat diesen Nachweis zu erbringen, was in der Realität oft nicht einfach sein dürfte, weil meist unklar ist, wer oder was in einem KI-System zu finden ist bzw. wer welche Datenbearbeitung vorgenommen hat.[69]

[49] Wie der Verantwortliche im Einzelfall seiner Auskunftspflicht nachzukommen vermag, ist technisch noch wenig geklärt;[70] vorgenommene Tests haben nicht wirklich befriedigende Resultate bzw. konkrete Antworten z.B. von ChatGPT gebracht.[71] Oft dürfte der Anbieter eines KI-Systems die Auskunft geben, dass keine Personendaten gesammelt worden seien, mangels Transparenz fehlt dem KI-Nutzer indessen der Einblick in das KI-System und das Auskunftsbegehren droht in die Leere zu laufen. Würde in Betracht gezogen, die Auskunft auf alle bisher generierten Antworten zur betroffenen Person in einem bestimmten KI-System zu erstrecken, wären, jedenfalls wenn es ich um ein grosses System handelt, die entsprechenden Antworten nicht oder nur beschränkt verfügbar, weil die Aufbewahrungszeit typischerweise relativ kurz ist.[72]

66 Vgl. auch Seiler/Griesinger (Fn. 5), Rz. 33–35 und Rosenthal (Fn. 4), Rz. 55 ff.

67 Weber (Fn. 1), S. 22.

68 Vgl. Rosenthal (Fn. 4), Rz. 57.

69 Rosenthal (Fn. 4), Rz. 59 f.; leicht relativierend Thouvenin/Volz (Fn. 5), S. 6.

70 Vgl. auch Chantal Lutz/Benjamin Domenig/Anja Flükiger, Datenschutzkonformer Einsatz von ChatGPT an Schulen, sic! 2024, S. 94, S. 96.

71 Rosenthal (Fn. 4), Rz. 63.

72 Eingehender dazu Rosenthal (Fn. 4), Rz. 64 f.

4.3.2. Ansprüche auf Widerspruch und Korrektur

[50] In der Praxis einfacher durchzusetzen sind die Widerspruchs- und Korrekturansprüche (Recht auf Vergessen).[73] Gewisse Anbieter, z.B. OpenAI für Chat-GPT, stellen ein entsprechendes Formular auf der Webseite zur Verfügung.[74] Hernach wäre über das Mittel des Auskunftsrechts zu prüfen, ob die Löschung auch wirklich durchgeführt worden ist.[75]

[51] Alternativ zur Löschung erscheint es als denkbar, dass der Anbieter des KI-Systems mittels technischer Massnahmen sicherstellt, dass die betroffenen Personendaten im «Output» des Systems nicht mehr vorkommen; damit wird derselbe Zweck erreicht wie mit der tatsächlichen Löschung.[76]

5. Ausblick

[52] Angesichts der vorerwähnten, nicht zu vernachlässigenden Rechtsunsicherheiten im Verhältnis zwischen Datenschutz und KI erscheint es als sinnvoll, wenn sich Anbieter und Betreiber von KI-Systemen, die Personendaten verarbeiten, eine Checkliste bereitlegen, um die DSG-Herausforderungen möglichst weitgehend erfüllen zu können. Folgende Fragen sind insbesondere für Betreiber mittlerer und grosser KI-Systeme relevant:[77]

- Verarbeitet das KI-System auch Personendaten?
- Ist die Funktionsweise des KI-Systems nachvollziehbar?
- Ersetzt das KI-System ein anderes System?
- Kann das KI-System direkt oder indirekt negative Auswirkungen auf besonders schützenswerte Personendaten haben?
- Wird der Grundsatz der Datenminimierung eingehalten?
- Ist die datenschutzrechtliche Rollenverteilung klar festgelegt?
- Nimmt das KI-System automatisierte Einzelentscheidungen vor?
- Wird ein Large Language Model in der Datenbearbeitung verwendet?
- Erhält der Nutzer adäquate Informationen über den Einsatz von KI-Programmen?
- Auf welcher Grundlage erfolgt der Einsatz des KI-Systems?
- Ist der Einsatz des KI-Systems überhaupt grundrechtskonform möglich?
- Liegen transparente und nachvollziehbare Informationen über die Algorithmen vor?
- Sind angemessene Datensicherheitsvorkehren eingerichtet?
- Werden die Grundsätze der «Privacy by Design» und der «Privacy by Default» eingehalten?
- Ist die Vornahme einer Datenschutz-Folgeabschätzung nötig? Wenn ja, wird sie durchgeführt?

---

73 Vgl. auch Thouvenin/Volz (Fn. 5), S. 6.

74 Vgl. https://share.hsforms.com/1UPy6xqxZSEq.TrGDh4ywo_g4sk30.

75 Vgl. auch Lutz/Domenig/Flükiger (Fn. 70), S. 96.

76 Rosenthal (Fn. 4), Rz. 64.

77 Vgl. auch Hans-Jürgen Pollirer, Checkliste Künstliche Intelligenz und Datenschutz, Datenschutz konkret 4/2023, S. 87, S. 89 f.

- Erfolgt die Erfüllung der Informationspflichten sachgerecht?
- Können die Auskunfts- und Widerspruchsrechte der Betroffenen eingehalten werden?

[53] Die Beachtung einer solchen Checkliste bedeutet nicht, dass die DSG-Komptabilität eines KI-Systems zweifelsfrei sichergestellt ist, aber zumindest wird ein sinnvoller Beitrag zur DSG-Vereinbarkeit der Bearbeitung von Personendaten geleistet. Wichtig ist in jedem Fall, dass der Betreiber eines KI-Systems intern Vorsorge trifft, dass sich die Mitarbeitenden der Datenschutz-Problematik bewusst sind und entsprechend handeln. Das Schweizer DSG statuiert nicht unüberwindbare Hürden (jedenfalls weniger als die DSGVO im grenzüberschreitenden Datenverkehr); mit angemessenen Datenschutzvorkehren lassen sich KI-Systeme durchaus erfolgreich nutzen.

Prof. Dr. Rolf H. Weber, Professor für internationales Wirtschaftsrecht an der Universität Zürich, dort Co-Leiter des «Center for Information Technology, Society, and Law» und des «Blockchain Center» sowie Rechtsanwalt in Zürich (Bratschi AG). Alle Internetseiten wurden zuletzt geprüft am 17. Juni 2024.