Universität Zürich[UZH]

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Rechtliche Auslegeordnung zur Entwicklung und Nutzung von KI im Bildungsraum Schweiz

Prof. Dr. Florent Thouvenin

Dr. Stephanie Volz

unter Mitarbeit von MLaw Deborah De Col, RA

Zürich, 21. August 2024

«Die Schlussfolgerungen des Berichts geben die Auffassung der Autoren wieder und entsprechen nicht zwingend denjenigen des Staatssekretariats für Bildung, Forschung und Innovation (SBFI) und der Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren (EDK) als Auftraggeber der Entwicklung einer Datennutzungspolitik für den Bildungsraum Schweiz.»

Inhaltsverzeichnis

EXECUTIVE SUMMARY

Künstliche Intelligenz (KI) hat grosses Potenzial, den Bildungssektor zu verändern. Der Einsatz dieser Technologie ist aber mit verschiedenen Herausforderungen verbunden. Der Begriff KI wird heute sehr weit gefasst. In diesem Bericht liegt der Fokus auf *machine-learning*-Systemen, deren wesentliches Merkmal darin besteht, dass sie nicht von Menschen vorgegebenen Regeln folgen. Stattdessen entwickeln sie eigenständig Regeln, indem sie statistische Muster in Daten erkennen, um vom Input zum Output zu gelangen. Dadurch sind sie in der Lage, andere Zusammenhänge zu erkennen und andere Analysen durchzuführen als Menschen oder klassische Algorithmen. Der konkrete Weg eines KI-Systems vom Input zum Output ist für Menschen jedoch nicht erklärbar und nachvollziehbar.

Eine grundlegende Frage beim Einsatz von KI im Bildungsbereich ist diejenige nach der datenschutzrechtlichen **Verantwortlichkeit**. Bei der Verwendung von KI-Tools wird in der Regel die Schule als Verantwortliche, der Anbieter des KI-Tools und ein allfälliger Cloud-Anbieter als Auftragsbearbeiter zu qualifizieren sein.

Zentral ist auch die Frage nach der **gesetzlichen Grundlage**. Staatliches Handeln bedarf immer einer gesetzlichen Grundlage. Das gilt auch im Datenschutzrecht. Eine Grundlage in einem Gesetz im formellen Sinn ist für die Bearbeitung von besonders schützenswerten Personendaten und teilweise für ein Profiling erforderlich. Die gesetzliche Grundlage legt auch den **Zweck der Datenbearbeitung** fest, denn Daten dürfen nur für den im Gesetz vorgesehenen Zweck bearbeitet werden (**Grundsatz der Zweckbindung**).

In den **Schulgesetzen** finden sich vielfach Ermächtigungen zur Bearbeitung von (besonders schützenswerten) Personendaten, die der Erfüllung einer öffentlichen Aufgabe der Schule dienen, wobei diese Ermächtigungen zumeist recht allgemeiner Art sind. Diese gesetzlichen Grundlagen dürften jedoch ausreichen, sofern die Datenbearbeitung durch ein KI-Tool der Erfüllung einer öffentlichen Aufgabe dient. Dies kann bspw. der Fall sein, wenn die Schule ein KI-Tool zum personalisierten Lernen einsetzt, denn der Bildungsauftrag der Schule umfasst in der Regel auch die individuelle Förderung der Schüler:innen.

Schwieriger ist die Frage zu beantworten, ob Personendaten als Trainingsdaten für die (Weiter-)Entwicklung von KI-Tools verwendet werden dürfen. In Bezug auf die Verbesserung von KI-Tools durch Schulen kann eine Verwendung als zulässig erachtet werden. Die Verwendung von Personendaten für das Training und die Weiterentwicklung durch den Anbieter des KI-Tools für eigene (kommerzielle) Zwecke dürfte hingegen nicht von der gesetzlichen Grundlage erfasst sein. Sofern der Anbieter des KI-Tools die Daten für eigene Zwecke nutzen möchte, liegt eine **Zweckänderung**, mindestens jedoch eine **Bekanntgabe an einen Dritten** vor. Eine solche ist nur zulässig, wenn eine

gesetzliche Grundlage besteht, eine Einwilligung im Einzelfall vorliegt, die Bekanntgabe für nicht personenbezogene Zwecke erfolgt oder die Daten anonymisiert werden. Eine gesetzliche Grundlage dürfte regelmässig fehlen, auch der Rechtfertigungsgrund der Einwilligung im Einzelfall dürfte nicht zum Tragen kommen, weil kein **Einzelfall** vorliegt, wenn standardmässig und über längere Zeit Daten über eine Vielzahl von Personen an einen KI-Anbieter übermittelt werden. Des Weiteren ist das Einholen einer Einwilligung nicht praktikabel, da eine wirksame Einwilligung an eine Reihe von Voraussetzungen, bspw. die jederzeitige Widerrufbarkeit der Einwilligung, geknüpft ist. In Konstellationen, in denen ein Subordinationsverhältnis besteht, wie dies zwischen der Schule und den Schüler:innen der Fall ist, ist zudem fraglich, ob eine Einwilligung überhaupt freiwillig sein kann. Eine Bekanntgabe der Daten an den Entwickler eines KI-Tools ist jedoch zulässig, sofern das kantonale Recht die Möglichkeit vorsieht, Personendaten zu nicht-personenbezogenen Zwecken, bspw. für Forschung, Planung oder Statistik, an Dritte weiterzugeben. Allerdings setzt dies voraus, dass die Bearbeitung von Personendaten für das Trainieren und Weiterentwickeln von KI als nicht personenbezogene Bearbeitung klassifiziert wird. Diese Auffassung erscheint zwar richtig; in dieser Frage besteht derzeit aber eine beträchtliche Rechtsunsicherheit. Eine Klärung der Rechtslage durch den Gesetzgeber oder durch die eidgenössischen oder kantonalen Aufsichtsbehörden wäre wünschenswert.

Die Verwendung von Daten zur (Weiter-)Entwicklung eines KI-Tools kann unter Umständen eine **Sekundärnutzung** darstellen, d.h. eine Verwendung von Daten zu einem anderen als dem gesetzlich vorgesehenen Zweck. Eine solche Nutzung ist ohne einschlägige gesetzliche Grundlage lediglich in Ausnahmefällen zulässig. Als Möglichkeit ist bspw. im Kanton Zürich das Einholen einer Einwilligung im Einzelfall zu nennen, was aus den genannten Gründen allerdings nicht praktikabel sein dürfte. Ähnlich wie die Bekanntgabe von Daten an Dritte ist auch die Bearbeitung von Daten für nicht personenbezogene Zwecke auf Bundes- und oft auch auf Kantonsebene zulässig. Darunter kann auch die Verwendung von Daten aus KI-Tools für die Weiterentwicklung durch den Anbieter des KI-Tools für eigene Zwecke fallen. Denkbar wäre auch, die Daten zu anonymisieren; damit käme das Datenschutzgesetz nicht mehr zur Anwendung.

Beim Einsatz von KI-Tools ist insbesondere darauf zu achten, dass die Vorgaben des Grundsatzes der **Verhältnismässigkeit** eingehalten werden, namentlich der Teilgehalt der **Datenminimierung**. Dieser steht in einem grundlegenden Spannungsverhältnis zur Funktionsweise von KI-Tools, die in der Regel umso besser funktionieren, je mehr Daten sie bearbeiten. Es muss deshalb jeweils im Rahmen einer Interessenabwägung geprüft werden, ob der Zweck der Datenbearbeitung die Menge der bearbeiteten Daten zu rechtfertigen vermag.

Gewisse Entscheidungen, die von Schulen getroffen werden, sind je nach Kanton als anfechtbare Verfügungen zu qualifizieren. Dazu gehören bspw. (promotionsrelevante) Leistungsbeurteilungen von Schüler:innen oder Schul- und Klassenzuteilungen. **Anfechtbare Verfügungen** sind – zumindest auf Nachfrage – zu begründen. Da KI-Systeme auf Korrelationen beruhen und nicht auf Kausalitäten, sind

die Entscheide dieser Systeme für Menschen nicht nachvollziehbar und sie lassen sich nicht in genügender Weise rechtlich begründen. Solange es nicht möglich ist, die für die Entscheidungen von KI-Tools relevanten Kriterien zu identifizieren, sind KI-Tools für Entscheide, die als Verfügungen ergehen, nicht geeignet.

Gewisse Entscheidungen von KI-Tools sind als **automatisierte Einzelentscheidungen** zu qualifizieren, wenn sie die betroffenen Personen erheblich beeinträchtigen. Das ist namentlich bei Promotionsentscheiden und teilweise auch bei Schul- und Klassenzuteilungen der Fall. Für automatisierte Einzelentscheidungen gelten (teilweise) besondere gesetzliche Vorgaben. Namentlich müssen die betroffenen Personen informiert werden, dass eine Entscheidung automatisiert gefällt wurde. Gestützt auf das datenschutzrechtliche Auskunftsrecht können die Betroffenen zudem verlangen, dass sie über die Logik informiert werden, die der automatisierten Entscheidung zugrunde liegt. Die Betroffenen müssen damit über den Einsatz eines KI-Tools und (auf Nachfrage) über die Funktionsweise des Algorithmus und die dem KI-Tool vorgegebenen Ziele sowie über die Datenkategorien informiert werden, die als Trainingsdaten verwendet wurden. Diese Information muss adressatengerecht erfolgen.

A. EINLEITUNG UND AUFTRAGSGEGENSTAND

Das Center for Information, Technology, Society, and Law (ITSL) wurde von Educa damit beauftragt, anhand von konkreten Use Cases eine rechtliche Auslegeordnung zur Entwicklung und Nutzung von Künstlicher Intelligenz (KI) im Bildungsraum Schweiz zu verfassen. Der vorliegende Bericht beleuchtet die rechtlichen Aspekte beim Einsatz von KI bei vier Use Cases; der Fokus liegt dabei auf datenschutz-rechtlichen Fragen. Der Bericht konzentriert sich auf die Perspektiven «Lehren und Lernen», «Schul-organisation» und «Anwendung in der Zukunft» und beschränkt sich dabei auf die Analyse der Zulässigkeit der Verwendung von KI. Nicht Gegenstand des Berichts ist die Frage, ob und inwieweit die heutigen analogen und digitalen Datenbearbeitungen den gesetzlichen Anforderungen genügen.

Der Begriff KI wird heute sehr weit gefasst. Als KI werden hier in Anlehnung an die Definition der OECD[1] und der KI-Verordnung der EU[2] maschinenbasierte Systeme verstanden, die für bestimmte von Men-schen definierte Ziele Voraussagen machen, Empfehlungen abgeben oder Entscheidungen treffen können, die das reale oder virtuelle Umfeld beeinflussen. KI-Systeme können mit einem unterschied-lichen Grad an Autonomie ausgestattet sein, der von einfachen assistierenden Funktionen bis hin zu vollständig autonomen Entscheidungen reicht, abhängig von ihrem Design, ihrer Anwendung und den ethischen Rahmenbedingungen.

In diesem Bericht liegt der Fokus auf *machine-learning*-Systemen, deren wesentliches Merkmal darin besteht, dass sie nicht von Menschen vorgegebenen Regeln folgen, sondern durch das **Erkennen statistischer Zusammenhänge** in Daten selbst Regeln entwickeln, um von einem Input zu einem Output zu gelangen. Dadurch sind diese Systeme in der Lage, mehr und andere Zusammenhänge zu erkennen und Analysen durchzuführen, als dies für Menschen oder klassischen Algorithmen möglich wäre. Der konkrete Weg eines KI-Systems vom Input zum Output ist für Menschen jedoch nicht erklärbar und nachvollziehbar.

Die rasch fortschreitende Entwicklung von KI hat das Potenzial, den Bildungssektor zu verändern, indem die Technologie bspw. individualisiertes Lernen ermöglicht und Lehrpersonen bei wieder-kehrenden Aufgaben unterstützt. Eine Vielzahl KI-unterstützter Tools ist bereits in Schulen im Einsatz. Neben diesen Chancen ist der Einsatz von KI-basierten Technologien auch mit Herausforderungen verbunden, insb. im Hinblick auf den Umgang mit persönlichen Daten von Schüler:innen, Lehrpersonen und Erziehungsberechtigten.

---

1 OECD (2019), Empfehlung des Rats zu künstlicher Intelligenz, OECD, Paris, «http://www.oecd.org/berlin/presse/Empfehlung-des-Rats-zu-kuenstlicher-Intelligenz.pdf».

2 Art. 3 lit. 1 Verordnung EU 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

Vor der weiteren Verwendung von KI sind die rechtlichen Implikationen dieser Technologie im Bildungsbereich zu untersuchen. Im Vordergrund steht dabei die Einhaltung der Vorgaben des Datenschutzrechts, weil KI grosse Mengen von Personendaten von Schüler:innen, Lehrpersonen und Erziehungsberechtigten bearbeitet.

B. LEHREN UND LERNEN: USE CASE 1: PERSONALISIERTES LERNEN UND KI-ASSISTENZ

KI bietet Möglichkeiten zur Verbesserung von Lehr- und Lernprozessen, insb. durch eine Personalisierung. Beim **personalisierten Lernen** werden Lerninhalte auf Basis der Interaktion von Schüler:innen mit einem KI-System an ihre persönlichen Bedürfnisse angepasst. Personalisiertes Lernen kann zu einer **KI-Assistenz** ausgebaut werden, die den Lernbedarf der Schüler:innen erkennt und entsprechend individualisierte Aufgaben stellen kann. Eine KI-Assistenz ist ein personalisiertes KI-Modell, das ein Individuum durch seine gesamte Bildungslaufbahn begleitet oder zumindest fächerübergreifend eingesetzt wird. Denkbar wäre, die KI-Assistenz so zu gestalten, dass sie **Persönlichkeitsmerkmale oder Emotionen** anhand von Merkmalen wie bspw. Handschrift, Sprache oder Videoaufnahmen erkennen kann.

Bei der datenschutzrechtlichen Beurteilung von KI-Tools ist zwischen der **Entwicklungsphase** und der **Anwendungsphase** zu unterscheiden. In der Praxis dürften Schulen häufig vollständig trainierte KI-Tools erwerben. Denkbar ist aber auch, dass eine Schule allein oder gemeinsam mit einem KI-Anbieter ein eigenes KI-Tool (weiter-)entwickelt und (weiter-)trainiert. Bei der datenschutzrechtlichen Beurteilung ist zwischen Trainingsdaten, Inputdaten und Outputdaten zu unterscheiden. Trainingsdaten kommen in der Entwicklungsphase zum Einsatz, Input- und Outputdaten bei der Anwendung, wobei Input- und Outputdaten auch zur Weiterentwicklung von KI-Tools genutzt werden können.

1. Anwendbarkeit der Datenschutzgesetze und betroffene Daten

Wird das KI-Tool von der Schule allein oder in Zusammenarbeit mit dem Anbieter eines KI-Tools trainiert, werden unter Umständen Daten von Schüler:innen als Trainingsdaten für das Modell genutzt. Im Rahmen des **personalisierten Lernens** und bei der **KI-Assistenz** werden Daten von Schüler:innen (und andere Daten) in ein KI-System eingegeben und von diesem analysiert. Die Inputs erfolgen über eine graphische Benutzeroberfläche oder durch Texteingabe, können aber auch handschriftlich oder per Sprache erfolgen. Denkbar ist auch, dass die Inputs aus verschiedenen Quellen, Lernaktivitäten, Beurteilungen durch Lehrpersonen und Erziehungsberechtigten stammen und so ein ganzheitliches Bild zu den Fähigkeiten, Fortschritten, Schwachstellen und Vorlieben einer/einem Lernenden ermöglichen.

Das eidgenössische Datenschutzgesetz (DSG) ist anwendbar, wenn Personendaten durch Private oder Bundesorgane bearbeitet werden. Die Bearbeitung durch kantonale öffentliche Organe (bspw. die Schulen) untersteht dem jeweiligen kantonalen Datenschutzgesetz.[3] Die Datenschutzgesetze regeln die Bearbeitung von **Personendaten**, also allen Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen. Die Bestimmbarkeit ist relativ, also aus Sicht des jeweiligen Bearbeitenden zu beurteilen; entscheidend ist, ob der Bearbeitende die Möglichkeit und ein Interesse daran hat, den Personenbezug herzustellen. Eine bloss theoretische Möglichkeit der Identifizierung reicht dafür nicht aus.[4] Liegt ein Personenbezug vor, muss die für die Datenbearbeitung verantwortliche Person, etwa ein Unternehmen oder ein öffentliches Organ, die Vorgaben des Datenschutzrechts einhalten. Fehlt der Personenbezug oder wird er nachträglich aufgehoben (**Anonymisierung**), so ist das Datenschutzrecht nicht anwendbar und die Bearbeitung der entsprechenden Daten ist in der Schweiz, von wenigen Ausnahmen abgesehen, nicht geregelt. Da eine Re-Identifikation mit den heutigen technischen Mitteln immer einfacher wird, sollte die Anonymisierung nicht leichthin angenommen werden.[5]

In der **Entwicklungsphase** ist es je nach KI-Tool möglich, das Tool mit anonymisierten Daten zu trainieren, so dass die Datenschutzbestimmungen keine Anwendung finden. Auch die Verwendung von synthetischen Daten, die keinen Personenbezug aufweisen, ist denkbar.[6] Viele Modelle werden aber für das Training Personendaten von Schüler:innen benötigen, womit die Vorgaben des Datenschutzrechts bei der Entwicklung von KI-Tools einzuhalten sind.

Bei der Anwendung bearbeiten KI-Tools **Inputdaten**, bspw. Sprachaufnahmen oder Texte der Schüler:innen, um ein personalisiertes Lernmodell zu erstellen. Diese Inputdaten sind als Personendaten zu qualifizieren, wenn sich die Schüler:innen aus ihnen bestimmen lassen. Solange die Daten nur lokal auf dem Gerät der Schülerin/des Schülers bearbeitet werden und Lehrpersonen, Anbieter des KI-Tools oder Dritte keine Möglichkeit haben, auf die Daten zuzugreifen, wird die Datenschutzgesetzgebung in der Regel nicht zur Anwendung gelangen, weil keine Bearbeitung von Personendaten durch einen Dritten vorliegt. In der Regel wird allerdings ein Anbieter von KI-Tools

---

3 Vorliegend wird im Wesentlichen auf die Rechtslage im Kanton Zürich abgestellt, punktuell wird auf die Rechtslage in anderen Kantonen verwiesen. Die anwendbaren kantonalen Datenschutzgesetze sind im Kanton Zürich das Gesetz über die Information und den Datenschutz (IDG/ZH), im Kanton Bern das (kantonale) Datenschutzgesetz (KDSG/BE), im Kanton Fribourg das Gesetz über den Datenschutz (DSchG/FR).

4 BSK DSG- BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, Art. 5 N 30.

5 BAERISWYL BRUNO, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz - Gegenseitige Herausforderungen, Zürich 2014, 51 ff; SHK DSG-RUDIN, Art. 5 N 13; BSK DSG- BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, Art. 5 N 35.

6 HAASE MARTIN S., Rechtmässigkeit der Benutzung personenbezogener Daten zum Trainieren künstlicher Intelligenz nach den Vorschriften der Datenschutz-Grundverordnung, InTeR 2023, 66 ff., 69; HACKER PHILIPP, A Legal Framework for AI Training Data - From First Principles to the Artificial Intelligence, 13 Law, Innovation and Technology (2021), abrufbar unter «https://ssrn.com/abstract=3556598», 9.

Zugang zu den Daten benötigen, um auf allfällige Probleme reagieren zu können. Auch Lehrpersonen dürften regelmässig Zugang zu gewissen Daten haben, um die Leistungen der Schüler:innen zu überprüfen und Einblick in die Funktionsweise des KI-Systems zu nehmen.

Aus den Inputdaten generiert das KI-Tool durch Analyse einen **Output**, der sich auf die individuellen Schüler:innen bezieht. Die Analyse der Leistung, des Lernfortschritts und der Leistungshistorie zur Zuweisung personalisierter Lerninhalte ist eine Bearbeitung von Personendaten, wenn eine Lehrperson Zugriff auf die Analysen und personalisierten Lernmodelle hat und diese Daten Rückschlüsse auf die einzelnen Schüler:innen zulassen. Aus Sicht des Anbieters des KI-Tools liegen dagegen nur dann Personendaten vor, wenn er die Daten einer/einem bestimmten Schüler:in zuordnen kann. Da das Interesse des Anbieters an der Bestimmbarkeit der einzelnen Schülerin/des einzelnen Schülers in aller Regel gering sein dürfte, werden die Daten – bei geeigneter Ausgestaltung der Modelle – aus Sicht des Anbieters regelmässig nicht als Personendaten zu qualifizieren sein.

Zusammenfassend lässt sich sagen, dass bei allen Formen des personalisierten Lernens zumindest teilweise Personendaten bearbeitet werden und daher die Vorgaben der jeweiligen Datenschutzgesetze einzuhalten und insb. die Grundsätze der Datenbearbeitung zu beachten sind.[7]

Besondere Anforderungen gelten, wenn **besonders schützenswerte Personendaten** (auch: besondere Personendaten[8]) bearbeitet werden oder ein **Profiling** erfolgt. Beim Einsatz von KI-Tools für das personalisierte Lernen wird eine Vielzahl von Personendaten erhoben. Bei einem KI-Assistenten zur Analyse von Fähigkeiten, Fortschritten und Ähnlichem können neben gewöhnlichen Personendaten auch besonders schützenswerte Personendaten bearbeitet werden. Erfolgt die Eingabe bspw. durch Handschrift oder Stimme, kann es sich um biometrische Daten handeln. Biometrische Daten gelten als besonders schützenswerte Personendaten, wenn sie mit einem spezifischen technischen Verfahren aus physischen, physiologischen oder verhaltensbezogenen Merkmalen einer Person gewonnen werden.[9] Diese Merkmale müssen eine eindeutige Identifizierung der Schüler:innen ermöglichen oder eine bereits bestehende Identifizierung bestätigen. Aus der Stimme können Algorithmen neben Alter, Geschlecht und Ethnie auch Gesundheitsdaten wie z.B. Angststörungen ableiten. Darüber hinaus kann aus der Stimme und dem Bildmaterial auf Charaktereigenschaften geschlossen werden, bspw. wie neugierig, konzentriert oder ausgeglichen die Schüler:innen sind und welche Emotionen sie haben.[10] Auch der **Output** von KI-Systemen kann aus besonders schützenswerten Personaldaten bestehen, insb. bei der KI-Assistenz. Zu denken ist etwa an Gesundheitsinformationen wie Diagnosen (bspw.

---

7 Siehe dazu hinten, B.3.

8 Bspw. Kanton ZH, § 3 Abs. 4 IDG/ZH.

9 Botschaft DSG 2017, BBl 2017 6941 ff., 7020; BSK DSG-BLECHTA/DAL MOLIN/WESIAK-SCHMIDT, Art. 5 N 65.

10 EVA WOLFANGEL, Unsere Stimme haben sie, digma 2019, 28 ff., 30.

Legasthenie oder Dyskalkulie). KI-Assistenten, die Persönlichkeitsmerkmale oder Emotionen erkennen sollen, werden immer besonders schützenswerte Personendaten bearbeiten.

Profiling liegt vor, wenn Informationen über eine Person automatisiert bearbeitet werden, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen (§ 3 Abs. 4 lit. c IDG/ZH). Das ist beim personalisierten Lernen häufig und bei der KI-Assistenz immer der Fall. Hier werden unterschiedliche Lerndaten, manchmal fächerübergreifend, innerhalb und ausserhalb der Schule und über einen längeren Zeitraum gesammelt und mit KI-Tools analysiert, wodurch ein ganzheitliches Bild der Fähigkeiten, Fortschritte und Vorlieben der Schüler:innen entsteht. In den meisten Fällen wird es sich sogar um ein Profiling mit hohem Risiko handeln, da solche Analysen mit einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen verbunden sind. Dies gilt insb. für KI-Assistenzsysteme, die neben Lerndaten auch Persönlichkeitsaspekte analysieren, indem sie bspw. Aussagen über eine Lernschwäche treffen können.

In der Regel bedarf die Bearbeitung von besonders schützenswerten Personendaten oder die Erstellung eines Profilings (mit hohem Risiko) durch ein staatliches Organ einer **Grundlage in einem Gesetz im formellen Sinn**. Zudem wird oft verlangt, dass vor der Bearbeitung eine **Datenschutzfolgenabschätzung** durchgeführt wird.

2. Beteiligte und Verantwortlichkeit

2.1. Verantwortlichkeit und Auftragsbearbeitung

Eine grundlegende Frage ist die Zuweisung der datenschutzrechtlichen **Verantwortlichkeit**. Für die Bearbeitung von Personendaten ist als Verantwortlicher zu qualifizieren, wer allein oder gemeinsam mit anderen über den **Zweck und die Mittel** der Bearbeitung entscheidet. **Auftragsbearbeiter** ist demgegenüber, wer Personendaten im Auftrag eines Verantwortlichen bearbeitet. Wer (allein oder gemeinsam) als Verantwortlicher und wer allenfalls als Auftragsbearbeiter zu qualifizieren ist, hängt von der konkreten Konstellation ab und kann nur im Einzelfall beurteilt werden.

Wenn der Anbieter eines KI-Tools dieses mit seinen eigenen Daten trainiert, ist er allein für die mit der Entwicklung verbundene Datenbearbeitung verantwortlich. Auch die Schule ist allein Verantwortliche bezüglich der Trainingsdaten, wenn sie ein KI-Tool selbst entwickelt. Entwickelt die Schule das KI-Tool zwar nicht selbst, nimmt aber bereits in der Entwicklungsphase Einfluss auf die Ausgestaltung des KI-Tools, indem sie bspw. dem Anbieter Trainingsdaten zur Verfügung stellt, ist sie für die Trainingsdaten verantwortlich, da sie über **Zweck und Mittel** der Datenbearbeitung entscheidet. Der Anbieter des KI-Tools wird als **Auftragsbearbeiter** zu qualifizieren sein, da er mit der Datenbearbeitung keine eigenen Zwecke verfolgt und die Daten nur im Rahmen seiner Dienstleistung für die Schule bearbeitet. Damit ist die Schule für die Einhaltung der Vorgaben des Datenschutzrechts verantwortlich. Die Einbindung der Auftragsbearbeiter erfolgt über einen **(Auftragsbearbeitungs-)Vertrag**, der gewisse gesetzlich

vorgeschriebene **Mindestinhalte** aufweisen muss. Im Kanton Zürich finden sich relevante Bestimmungen bspw. in der Verordnung über die Information und den Datenschutz sowie in den Allgemeinen Geschäftsbedingungen des Regierungsrats für Informatikleistungen. Entsprechende (gleichwertige) Bestimmungen können aber auch individuell ausgehandelt werden. Nur wenn ein Anbieter überhaupt keine Datenbearbeitung vornimmt, weil die ihm zur Verfügung gestellten Daten **anonymisiert** sind, wird er zum unbeteiligten Dritten.

In der Regel verwenden Schulen vortrainierte KI-Tools von Drittanbietern, die sie über eine Schnittstelle des KI-Anbieters laufen lassen. Der Anbieter wird das System auf eigenen Servern oder auf der Cloud eines Dritten betreiben. Denkbar ist aber auch, dass eine Schule ein KI-System auf eigenen Servern betreibt. Je nach Konstellation sind mehrere Akteure beteiligt: Der Anbieter des KI-Systems, ein Cloud-Anbieter und die Betreiberin des Systems, also die Schule.

Bei mehreren Beteiligten kann die Frage der Verantwortlichkeit schwierig zu beantworten sein. Es lassen sich deshalb nur einige allgemeine Aussagen machen: Werden KI-Systeme auf fremden Servern genutzt und Personendaten als Inputdaten verwendet, ist die **Schule** als Betreiberin des KI-Systems für die Bearbeitung dieser Daten **verantwortlich**. Gleiches gilt für den Output des KI-Tools. Der **Anbieter des KI-Tools** ist als **Auftragsbearbeiter** zu qualifizieren. In der Anwendungsphase dürfte der Anbieter in den seltensten Fällen als unbeteiligter Dritter anzusehen sein, da hierfür die Input- und Outputdaten «Ende-zu-Ende» verschlüsselt werden müssten. Da die Daten zumindest bei der Umwandlung von Input zu Output als Klardaten vorliegen müssen, sind dieser Variante aus heutiger Sicht technische Grenzen gesetzt.

Wenn die Schule das System auf ihren eigenen Servern betreibt, ohne dass der KI-Anbieter Zugriff auf die Input- oder Outputdaten hat, ist die **Schule allein verantwortlich**. Der Anbieter des KI-Tools führt keine Datenbearbeitung durch und ist daher als unabhängiger Dritter zu qualifizieren. Da der Anbieter des KI-Tools zumindest zu Kontrollzwecken oder zur Fehlerbehebung Zugriff auf das System haben muss, dürfte auch diese Konstellation aktuell in der Praxis noch wenig verbreitet sein.

Besondere Fragen stellen sich, wenn KI-Tools in der **Cloud eines Drittanbieters** betrieben werden. Wenn Daten in einer Cloud gespeichert und bearbeitet werden, ist der Cloud-Anbieter als zusätzlicher **Auftragsbearbeiter** zu qualifizieren. Die Bearbeitung von Daten in der Cloud birgt höhere Risiken als eine Datenbearbeitung durch Dritte im herkömmlichen Sinn, weil in gewisser Weise die Kontrolle über die Daten verloren geht. KI-Tools, die Daten in der Cloud bearbeiten, müssen daher sorgfältig auf die Einhaltung der datenschutzrechtlichen Anforderungen geprüft werden. Zudem muss auch mit dem Cloud-Anbieter ein (**Auftragsbearbeitungs-**)**Vertrag** abgeschlossen werden, der den gesetzlich statuierten Mindestinhalten zu genügen hat. Besonders heikel wird es, wenn sich die Cloud in einem Land befindet, das aus Sicht der Schweiz keinen angemessenen Datenschutz gewährleistet. Dazu gehören die meisten aussereuropäischen Länder, insb. die USA. In diesem Fall sind besondere Vorkehrungen zu treffen. Da die Anbieter jedoch regelmässig einen Cloud-Standort in Europa zur

Verfügung stellen, werden die zu treffenden Massnahmen nicht näher erläutert. Handelt es sich, wie im Fall der KI-Assistenz, um besonders umfangreiche und sensible Datenbearbeitungen, sollte nach Möglichkeit eine Cloud in der Schweiz genutzt werden.

Zum **Verantwortlichen** könnte der **Anbieter des KI-Tools** nur werden, wenn er personenbezogene Input- oder Outputdaten für eigene Zwecke verwendet.

2.2. Bekanntgabe an Dritte

Beim personalisierten Lernen stellt sich die Frage, ob die Schulen dem Anbieter des KI-Tools Daten über die Schüler:innen bekannt geben dürfen, damit dieser das System für seine eigenen (kommerziellen) Zwecke (weiter-)entwickeln kann. Vier Möglichkeiten sind denkbar, damit eine Bekanntgabe von Daten zulässig ist: Es besteht (1) eine **gesetzliche Grundlage**, es liegt (2) eine **Einwilligung** im Einzelfall vor (§ 16 IDG/ZH, Art. 10 f. KDSG/BE, Art. 14 DSchG/FR)[11], die Bekanntgabe erfolgt (3) für nicht personenbezogene Zwecke oder (4) die Daten werden vor der Bekanntgabe anonymisiert, womit die Datenschutzgesetze nicht (mehr) zur Anwendung kommen.

Eine **gesetzliche Grundlage** für die Bekanntgabe dürfte regelmässig fehlen. Denkbar ist an sich das Einholen einer **Einwilligung im Einzelfall**. Dieser Rechtfertigungsgrund scheidet aber aus, weil kein **Einzelfall** vorliegt, wenn standardmässig und über längere Zeit Daten von einer Vielzahl von Personen an einen KI-Anbieter übermittelt werden. Das Einholen einer Einwilligung ist auch nicht praktikabel, weil eine wirksame Einwilligung an eine Reihe von Voraussetzungen geknüpft ist. Eine gültige Einwilligung liegt nur vor, wenn sie nach ausreichender Information freiwillig erteilt wird.[12] Ausserdem kann sie jederzeit widerrufen werden.[13] Die Einwilligung müsste von der Schule eingeholt werden. Die Schüler:innen stehen allerdings in einem Subordinationsverhältnis zur Schule, weshalb fraglich ist, ob eine allenfalls erteilte Einwilligung als freiwillig qualifiziert werden kann.[14] Auch die Widerrufsmöglichkeit ist in der Praxis schwer umsetzbar.

Einige Datenschutzgesetze sehen die Möglichkeit vor, Personendaten für **nicht personenbezogene Zwecke** bekannt zu geben, bspw. für Datenbearbeitungen für Forschung, Planung oder Statistik (bspw. § 18 IDG/ZH, Art. 26 DSchG/FR, Art. 15 KDSG/BE). Der Empfänger muss in diesen Fällen nachweisen, dass die Auswertungen keine Rückschlüsse auf die betroffenen Personen zulassen und dass er die ursprünglichen Daten nach der Anonymisierung vernichtet. Ob die Bestimmungen über die Bekannt-

---

11 Im Kanton Zürich gibt es noch die Möglichkeit der Bekanntgabe zur Abwendung einer drohenden Gefahr für Leib und Leben, dieser Fall dürfte jedoch vorliegend nicht einschlägig sein (§ 16 lit. c IDG/ZH). Im Kanton Bern können Daten auch bekannt gegeben werden, wenn die Bekanntgabe im Interesse der betroffenen Person ist (Art. 10 Abs. 1 lit. c und Art. 11 Abs. 1 lit. a KDSG/BE), im Kanton Fribourg beim Vorliegen von überwiegenden Interessen Privater (Art. 14 Abs. 2 lit. c DSchG/FR).

12 Siehe dazu Art. 6 Abs. 6 DSG; BSK DSG-BÜHLMANN/REINLE, Art. 6 N 277 ff.

13 BSK DSG-BÜHLMANN/REINLE, Art. 6 N 316; SHK DSG-BAERISWYL, Art. 6 N 84.

14 BSK DSG-BÜHLMANN/REINLE, Art. 6 N 286.

gabe für nicht personenbezogene Zwecke auf die Bekanntgabe von Personendaten an Anbieter von KI-Tools angewendet werden können, ist aus zwei Gründen unklar: Zum einen wird in der Lehre teilweise verlangt, dass bei einer Bearbeitung für nicht personenbezogene Zwecke die Auswertung der breiten Öffentlichkeit zugänglich gemacht wird.[15] Der Anbieter des KI-Tools wird aber die Daten für sich selbst bearbeiten und die Ergebnisse nicht öffentlich zugänglich machen wollen.[16] Die in der Lehre vertretene Auffassung orientiert sich allerdings an den Regelbeispielen der Bearbeitung für Forschung, Planung und Statistik und leitet daraus eine Voraussetzung für alle Formen der Bearbeitung für nicht-personenbezogene Zwecke ab, die sich so in den Datenschutzgesetzen nicht findet. Aus unserer Sicht steht der fehlende öffentliche Zugang der Auswertung einer Anwendung dieser Bestimmungen auf das Training von KI deshalb nicht entgegen.[17] Zum andern besteht noch kein Konsens, dass die (Weiter-)entwicklung eines KI-Tools als Bearbeitung für nicht personenbezogene Zwecke qualifiziert werden kann. Für das Vorliegen einer solchen Bearbeitung spricht, dass der Verantwortliche kein Interesse an einer Individualisierung der Daten hat und die Bearbeitung für die betroffenen Personen keinerlei Folgen hat; zudem sollte der Verantwortliche angemessene Massnahmen treffen, damit die Daten auch tatsächlich nicht individualisiert, also einer bestimmten Person zugeordnet werden können. Auch wenn diese Auffassung aus unserer Sicht richtig ist, besteht die Gefahr, dass eine Aufsichtsbehörde die Frage anders beurteilt. Um die bestehende Rechtsunsicherheit zu beheben, wäre eine Klärung der Rechtslage durch den Gesetzgeber oder die zuständigen Aufsichtsbehörden wünschenswert.

3. Datenbearbeitungsgrundsätze

3.1. Rechtmässigkeit

Personendaten dürfen nur rechtmässig bearbeitet werden. Im öffentlich-rechtlichen Bereich bedeutet der Grundsatz der Rechtmässigkeit, dass die Datenbearbeitung nur zulässig ist, wenn eine gesetzliche Grundlage besteht. Das gilt auch für die Bearbeitung von Personendaten durch Schulen. In einem ersten Schritt ist deshalb zu prüfen, ob sich die Schule für die Bearbeitung von Personendaten auf eine gesetzliche Grundlage stützen kann.

Für die Datenbearbeitung durch kantonale und kommunale Behörden gelten die kantonalen Datenschutzgesetze, im Kanton Zürich insb. das IDG/ZH, im Kanton Bern das KDSG/BE und im Kanton Fribourg das DSchG/FR. Da die Volksschulen kantonale öffentliche Organe sind, müssen sie die Vorgaben der kantonalen Datenschutzgesetze (IDG/ZH, KDSG/BE, DSchG/FR) einhalten. Ergänzend

---

15 BSK DSG-RAMPINI/HARASGAMA, Art. 31 N 60.

16 BSK DSG-RAMPINI/HARASGAMA, Art. 31 N 54.

17 Dazu White Paper Datenschutz, abrufbar unter «https://www.itsl.uzh.ch/de/Forschung-und-Beratung/Forschungsprojekte.html».

gelten kommunale Erlasse oder kantonale Erlasse wie Gemeindegesetze oder Volksschulgesetze. Viele Volksschulgesetze bzw. die dazugehörigen Verordnungen enthalten rechtliche Grundlagen für eine Reihe von Datenbearbeitungen (bspw. VSG/ZH und VSV/ZH). Diese sind jedoch in der Regel eher allgemein gehalten. Sie erlauben auch die Bearbeitung von (besonders schützenswerten) Personendaten, wenn dies der Erfüllung einer öffentlichen Aufgabe der Schule dient. Auch Schulkreise oder einzelne Schulen können sich auf bestimmte Rechtsgrundlagen für Datenbearbeitungen stützen.

Für die hier zu untersuchenden Fragen ist entscheidend, ob sich die rechtlichen Grundlagen, die den Schulen die Bearbeitung von Personendaten im Zusammenhang mit der individuellen Förderung erlauben, auch die Bearbeitung durch KI-Tools umfassen.

Die Gültigkeitsvoraussetzungen der hinreichenden **Normstufe und Normdichte** gelten auch für den Einsatz von KI-Tools und können grundsätzlich auf diese angewendet werden.[18] Das Erfordernis der genügenden Normstufe bedeutet, dass wichtige Eingriffe in die Persönlichkeit in einem Gesetz im formellen Sinn geregelt sein müssen, das Erfordernis der Normdichte verlangt, dass die Norm genügend bestimmt ist.[19] Hinsichtlich der Normdichte dürften die gesetzlichen Grundlagen, die die Datenbearbeitung zur Erfüllung des Bildungsauftrags regeln, in vielen Fällen auch den Einsatz von KI-Tools umfassen. Ob die Korrektur und Aufgabenzuteilung durch eine Lehrperson oder durch ein KI-Tool erfolgt, erscheint nicht relevant, zumal die Datenbearbeitung grundsätzlich dieselbe ist. Problematisch kann allerdings sein, dass ein KI-System in der Lage ist, deutlich mehr Daten über die Schüler:innen zu bearbeiten als eine Lehrperson. Zudem können solche Systeme Zusammenhänge erkennen und Schlussfolgerungen ziehen, die weit über die Fähigkeiten von Menschen oder anderen Systemen hinausgehen. Es könnte daher argumentiert werden, dass der Einsatz von KI grundlegend von der in der Rechtsgrundlage vorgesehenen Datenbearbeitung abweicht und deshalb eine eigene Rechtsgrundlage erforderlich ist.

Eine **ausdrückliche gesetzliche Grundlage** ist oft erforderlich, wenn besonders schützenswerte Personendaten bearbeitet werden oder ein Profiling vorliegt.[20] Das Erfordernis der Normstufe ist eingehalten, wenn die spezifische Befugnis für die Datenbearbeitung in einem **Gesetz im formellen Sinn** enthalten ist. Das ist der Fall, wenn die Regelung als Gesetz vom Parlament (als Legislative) und nicht von der Exekutive (etwa in Form einer Verordnung) erlassen wurde. Im Gesetz im formellen Sinn müssen dabei das zuständige öffentliche Organ, die Kategorien der Daten, die Bearbeitungsmethoden

---

18 PHILIP GLASS, Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung, Eine Auslegeordnung am Beispiel des Kantons Zürich, in: Michael Widmer (Hrsg.), Datenschutz: Rechtliche Schnittstellen, Zürich 2023, 177 ff.; 208.

19 BENJAMIN SCHINDLER, in: Bernhard Ehrenzeller/Patricia Egli/Peter Hettich/Peter Hongler/Benjamin Schindler/Stefan G. Schmid/Rainer J. Schweizer (Hrsg.), St. Galler Kommentar Schweizerische Bundesverfassung, 4. Auflage 2024, St. Gallen, Art. 5 N 34 ff.; GIOVANNI BIAGGINI, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. Auflage 2017, Zürich, Art. 5 N 9 ff.

20 So ausdrücklich im DSG, Art. 34 Abs. 2 lit. a – c; GLASS (Fn 18), 208.

und der Zweck der Bearbeitung normiert sein. Für die Bearbeitung «gewöhnlicher» Personendaten genügt hingegen eine von der Exekutive erlassene Verordnung, es sei denn, der Zweck oder die Art und Weise der Bearbeitung bergen ein besonderes Risiko für die Grundrechte der betroffenen Personen.[21]

Werden mit KI-Tools für das **personalisierte Lernen** gewöhnliche Personendaten bearbeitet, muss sich diese Datenbearbeitung zumindest implizit aus der öffentlichen Aufgabe der Schule ergeben. Werden besonders schützenswerte Personendaten bearbeitet, was zumindest bei **KI-Assistenten** regelmässig der Fall sein dürfte, muss für diese Datenbearbeitung eine explizite Grundlage in einem Gesetz im formellen Sinn bestehen. Im Kanton Zürich hält das Volksschulgesetz (VSG/ZH) fest, dass die zuständigen öffentlichen Organe zur Erfüllung ihrer Aufgaben nach dem VSG/ZH Personendaten und besonders schützenswerte Personendaten (inkl. Profiling) bearbeiten dürfen, bspw. Daten über die Religionszugehörigkeit, die Gesundheit und die Familienverhältnisse (siehe § 3a Abs. 2 VSG/ZH). Diese Bestimmung dürfte als Rechtsgrundlage für den Einsatz von KI-Assistenten genügen. Die Rechtslage kann jedoch von Kanton zu Kanton verschieden sein.

Das DSG und gewisse kantonale Gesetze[22] enthalten eine spezielle Bestimmung für **Pilotversuche**. Nach Art. 35 DSG kann der Bundesrat im Rahmen von Pilotversuchen die automatisierte Bearbeitung von besonders schützenswerten Personendaten und andere Datenbearbeitungen für eine befristete Versuchsphase zulassen oder auf Verordnungsstufe regeln. Dies ermöglicht die provisorische Einführung von KI-Tools, bis die erforderliche gesetzliche Grundlage vorliegt. Auch der Kanton Zürich wird im Rahmen der Revision des IDG/ZH voraussichtlich eine solche Pilotklausel einführen.[23]

3.2. Zweckbindung

Der Grundsatz der Zweckbindung gilt nicht nur auf Bundesebene, sondern auch nach den kantonalen Datenschutzgesetzen (§ 9 IDG/ZH, Art. 5 KDSG/BE, Art. 7 DSchG/FR). Im öffentlich-rechtlichen Bereich wird mit der gesetzlichen Grundlage für die Datenbearbeitung auch deren Zweck umschrieben. Daten dürfen demnach **nur zum im Gesetz vorgesehenen Zweck bearbeitet** werden.

Beim Einsatz von KI-Tools für das personalisierte Lernen bzw. Erstellen von personalisierten Lernmodellen liegt der Zweck der Datenbearbeitung in der Analyse des Lernfortschritts zur individuellen Förderung der Schüler:innen. Eine gesetzliche Grundlage, die diese Aufgabe als Bearbeitungszweck vorsieht, findet sich bspw. in § 2 Abs. 4 VSG/ZH. Danach gehört es zu den Bildungs- und Erziehungsaufgaben, im Unterricht die **individuellen Begabungen und Neigungen** der Kinder zu

---

21 Bspw. Art. 34 Abs. 2 lit. c DSG.

22 Demnächst das IDG/ZH, das aktuell revidiert wird, siehe dazu «https://www.zh.ch/de/news-uebersicht/medienmitteilungen/2023/08/kanton-zuerich-modernisiert-gesetz-ueber-information-und-datenschutz.html». Im Kanton Fribourg gilt Art. 22 DSchG und das E-Government Gesetz.

23 Vorentwurf mit erläuterndem Bericht, 4.

berücksichtigen. Zur Erfüllung dieser Aufgabe dürfen Daten über schulische Leistungen sowie das Lernverhalten bearbeitet werden.[24] Diese Aufgabe kann von der Schule auch mithilfe eines KI-Tools erfüllt werden. Der Einsatz des KI-Tools ist daher von der Zweckbestimmung gedeckt. Das gilt auch für die Bearbeitung von besonders schützenswerten Personendaten.

Weniger eindeutig ist die Rechtslage bei der Nutzung von Personendaten als **Trainingsdaten für die (Weiter-)Entwicklung** von KI-Tools. Unzulässig dürfte es sein, wenn Daten für das Training eines KI-Tools verwendet werden, die für einen völlig anderen Zweck erhoben wurden, bspw. Daten aus einer schulärztlichen Untersuchung. Wenn Daten für einen ähnlichen Zweck erhoben wurden, bspw. für das Erstellen von Arbeitsblättern oder für ein elektronisches Arbeitsdossier, ist die Verwendung als Trainingsdaten eher zulässig. Daten können in unterschiedlicher Weise für das Training eines KI-Tools verwendet werden. Bei der Verwendung von Schüler:innendaten zu Trainingszwecken ist daher im Einzelfall zu prüfen, welche Daten zu welchem Zweck verwendet werden dürfen. Bei der Nutzung von Daten zur Weiterentwicklung von KI-Tools ist zu unterscheiden: Wenn die von den Schüler:innen in das KI-Tool eingegebenen Daten zur Verbesserung des Systems genutzt werden und so der Erfüllung des Bildungsauftrages dienen, liegt keine Zweckänderung vor und die Nutzung ist zulässig. Die Weiterentwicklung durch den Anbieter des KI-Tools für eigene (kommerzielle) Zwecke dürfte hingegen nicht erfasst sein. Auch hier ist zur Beurteilung der Zulässigkeit auf den jeweiligen Einzelfall abzustellen. Diese Aussagen lassen sich auf alle Use Cases übertragen.

Eine Verwendung von Daten zu einem anderen als dem gesetzlich vorgesehenen Zweck (**Sekundärnutzung**) ohne einschlägige gesetzliche Grundlage ist nur in Ausnahmefällen möglich. Die Frage nach der zulässigen Sekundärnutzung stellt sich vor allem bei der Verwendung von Personendaten zur (Weiter-)Entwicklung des KI-Tools. Eine Sekundärnutzung ist in drei Fällen denkbar: (1) Es kann eine Einwilligung im Einzelfall eingeholt werden (bspw. § 9 IDG/ZH), (2) es liegt eine Bearbeitung für nicht personenbezogene Zwecke vor oder (3) die Daten wurden anonymisiert. Bezüglich der Problematik der Einwilligung kann auf die Ausführungen zur Bekanntgabe von Daten verwiesen werden.[25] Ähnlich wie die Bekanntgabe ist auch die Bearbeitung von Daten für nicht personenbezogene Zwecke auf Bundes- und Kantonsebene zulässig.[26] Die Verwendung von Daten aus KI-Tools für die Weiterentwicklung kann unter diese «nicht personenbezogenen Zwecke» fallen.[27]

---

24 Gemäss § 3a VSG/ZH bearbeiten die zuständigen öffentlichen Organe für die Erfüllung ihrer Aufgaben nach dem VSG Daten, einschliesslich Personendaten und besonders schützenswerter Personendaten von Schüler:innen (Abs. 1). Daten gemäss Abs. 1 sind insb. Informationen über schulische Leistungen, Arbeits-, Lern- und Sozialverhalten, sonderpädagogische Massnahmen, Disziplinarmassnahmen, Auszeiten und Religionszugehörigkeit, Gesundheit und Familienverhältnisse (Abs. 2).

25 Siehe dazu vorne, B.2.2.

26 Kanton Zürich: § 9 Abs. 2 IDG/ZH, Bund: Art. 39 DSG.

27 Siehe dazu vorne, B.3.2.

3.3. Verhältnismässigkeit, Datenminimierung

Nach dem Grundsatz der Verhältnismässigkeit darf die Bearbeitung von Personendaten nur so weit gehen, wie dies objektiv für einen bestimmten Zweck **geeignet und erforderlich** ist. Der Zweck muss zudem in einem **angemessenen Verhältnis** zum Eingriff in die Grundrechte der betroffenen Person stehen.[28] Die Verhältnismässigkeit sollte bei der Datenbearbeitung durch staatliche Organe bereits in der gesetzlichen Grundlage berücksichtigt werden. Sie spielt jedoch eine Rolle, wenn die gesetzliche Grundlage – was in den hier in Frage stehenden Konstellationen in der Regel der Fall sein dürfte – wenig spezifisch ist.[29]

Aus dem Grundsatz der Verhältnismässigkeit wird das Gebot der **Datenminimierung** abgeleitet, nach dem nur die Daten erhoben und bearbeitet werden dürfen, die für einen bestimmten Zweck tatsächlich erforderlich sind.[30] Da die Umsetzung der Datenminimierung je nach Situation unterschiedlich sein kann, ist es wichtig, im Einzelfall eine **Interessenabwägung** vorzunehmen und zu prüfen, welche Daten für den jeweiligen Zweck erforderlich sind.[31] Der Grundsatz der Verhältnismässigkeit gilt auch in zeitlicher Hinsicht. Daten dürfen deshalb nur so lange aufbewahrt werden, wie es für das Erreichen des Zwecks geeignet und erforderlich ist, sog. **Speicherbegrenzung**.[32] Die Datenminimierung ist besonders relevant, wenn es sich um grosse Datenmengen handelt, was normalerweise der Fall ist, wenn KI-Tools eingesetzt werden. Um dem Grundsatz zu genügen, dürfen nur Informationen über die Schüler:innen erfasst werden, die für das Erreichen des Zweckes notwendig sind. So ist es bspw. nicht notwendig, persönliche Einstellungen zu erfassen, die sich aus den vom KI-Tools analysierten Aufsätzen ergeben. Darüber hinaus kann durch technische Massnahmen verhindert werden, dass unnötige Daten erhoben werden, bspw. durch die Vermeidung unspezifischer Felder wie «Allgemeine Informationen».

Das Zusammenspiel der Grundsätze der Verhältnismässig und der Zweckbindung läuft darauf hinaus, dass die Erhebung und Speicherung von Daten ohne konkreten Bearbeitungszweck bzw. «auf Vorrat» unverhältnismässig und somit unzulässig ist.[33] Die Einhaltung dieser Grundsätze kann jedoch dem Interesse an datengetriebener Innovation zuwiderlaufen, weil diese häufig von der langfristigen Verfügbarkeit von Daten abhängt und Daten für Zwecke verwendet werden können, die zum Zeitpunkt ihrer Erhebung noch nicht bekannt waren. Namentlich für KI-Systeme, die sich auf das Erkennen von Korrelationen zwischen Daten konzentrieren, können alle in einem System vorhandenen Daten von

---

28 BSK DSG-BÜHLMANN/REINLE, Art. 6 N 53.

29 BSK DSG-BÜHLMANN/REINLE, Art. 6 N 58.

30 Ausdrücklich in Art. 6 Abs. 4 DSG; Botschaft DSG 2017, BBl 2017 6941 ff., 7026; BSK DSG-BÜHLMANN/REINLE, Art. 6 N 220.

31 BSK DSG-BÜHLMANN/REINLE, Art. 6 N 221.

32 SHK DSG-BAERISWYL, Art. 6 N 53; zur Speicherbegrenzung: DAMIAN GEORGE, Prinzipien und Rechtmässigkeitsbedingungen im privaten Datenschutzrecht, Diss. Zürich, 2021, 310 f.

33 GLASS (Fn 18), 209.

Bedeutung sein.[34] Auch diese Perspektive ist bei der Interessenabwägung zu berücksichtigen. Sie kann namentlich dazu führen, dass mehr Daten erhoben und die Daten länger gespeichert werden können, weil diese Daten für die Verwendung und die Weiterentwicklung von KI-Tools wichtig sind.

Im Bereich des personalisierten Lernens ist der **Grundsatz der Verhältnismässigkeit** von besonderer Bedeutung. KI-Tools, die personalisiertes Lernen nur innerhalb einer Bildungsstufe und innerhalb eines Faches bzw. einer Gruppe von Fächern einsetzen und die erhobenen Daten nach einer gewissen Zeit wieder löschen, entsprechen dem Grundsatz der Datenminimierung am ehesten. Allerdings muss auch hier sichergestellt werden, dass die erhobenen und ausgewerteten Daten zur Erfüllung des Bildungs- und Erziehungsauftrags geeignet und erforderlich sind. KI-Assistenten, die über die gesamte Laufbahn und fächerübergreifend eingesetzt werden, sind unter dem Gesichtspunkt der Datenminimierung heikler. Grössere Mengen von Daten können jedoch die Qualität und den Nutzen von KI-Tools erhöhen. Je mehr Daten aus einem breiten Spektrum von Aktivitäten gesammelt werden und je länger diese Daten bearbeitet werden, desto individueller kann das KI-Modell auf die Schüler:innen zugeschnitten werden und desto besser kann die öffentliche Aufgabe erfüllt werden. Es ist deshalb stets eine **Interessenabwägung** zwischen dem Persönlichkeitsschutz der Schüler:innen und dem zusätzlichen Nutzen der Bearbeitung der Personendaten vorzunehmen.

KI-Assistenten zur Erkennung von Persönlichkeitsmerkmalen und Emotionen bearbeiten neben gewöhnlichen auch besonders schützenswerte Personendaten. Beim Einsatz eines solchen Tools wäre im Einzelfall zu prüfen, welche Daten für das Erreichen des gesetzlich vorgesehenen Bearbeitungszwecks erforderlich sind. Dabei muss sichergestellt werden, dass Merkmale wie der Gesundheitszustand oder andere, für den Zweck des Tools nicht erforderliche Daten nicht erhoben werden, auch wenn dies technisch problemlos möglich wäre. KI-Tools dürfen also nicht alle möglichen physischen, physiologischen oder verhaltensbezogenen Merkmale erfassen, sondern nur diejenigen, die zur Erfüllung der gesetzlich vorgesehenen Aufgabe, für die sie eingesetzt werden, erforderlich sind. Auch bei der zusätzlichen Erfassung von Daten durch Dritte, bspw. Erziehungsberechtigte, ist zu prüfen, ob diese Datenbearbeitungen für das Erreichen des Bearbeitungszwecks erforderlich sind.

Bei der Beurteilung der Verhältnismässigkeit muss für jede spezifische Datenbearbeitung analysiert werden, ob sie notwendig ist, um das in der gesetzlichen Grundlage definierte Ziel zu erreichen und ob der mit der Datenbearbeitung verfolgte Nutzen in einem vernünftigen Verhältnis zum Eingriff in die Persönlichkeitsrechte der betroffenen Person steht.

3.4. Transparenz und Erkennbarkeit

Die Bearbeitung von Personendaten und der Bearbeitungszweck müssen für die betroffenen Personen **erkennbar sein.** Bei der Datenbearbeitung durch öffentliche Organe ergeben sich die Erkennbarkeit

---

[34] STEPHANIE VOLZ, KI-Sandboxen für die Schweiz?, SZW 2021, 51 ff., 56.

und die Transparenz der Datenbearbeitung aus der **gesetzlichen Grundlage**.[35] Wenn eine Datenbearbeitung auf einer gesetzlichen Grundlage beruht, entfällt deshalb die Informationspflicht (Art. 20 Abs. 1 lit. b DSG, § 12 Abs. 3 lit. b IDG/ZH).

Dennoch kann eine Information der betroffenen Schüler:innen und Eltern sinnvoll sein, namentlich um Vertrauen zu schaffen. Da sich die Informationsbedürfnisse der Schüler:innen und der Erziehungsberechtigten unterscheiden, sollten die Informationen in verschiedenen Formaten und auf verschiedenen Komplexitätsstufen angeboten werden, bspw. durch das Anbieten von einfachen und grundlegenden Informationen auf einer ersten Ebene und zusätzlichen vertiefenden Informationen, die bei Bedarf abgerufen werden können. Gerade bei jüngeren Schüler:innen kann es sinnvoll sein, die Informationen in Form von Bildern oder Videos anzubieten. Denkbar ist auch, den Erziehungsberechtigten den Zugang zu den KI-Tools zu ermöglichen, bspw. über einen Test-Account. So können sie nachvollziehen, wie die KI-Tools funktionieren und wie personalisierte Lernmodelle gestaltet sind.

3.5. Datenrichtigkeit

Nach dem Grundsatz der Datenrichtigkeit muss sich der Verantwortliche vergewissern, dass die Personendaten richtig sind. Falsche oder unvollständige Daten müssen korrigiert, gelöscht oder vernichtet werden. Falsche oder ungenaue Daten in einem personalisierten Lernmodell könnten direkte Auswirkungen auf das Profil einzelner Schüler:innen haben und sich auf die Bewertung der Schüler:innen durch die Lehrperson sowie auf die empfohlenen Lernressourcen auswirken.[36]

Das KI-Tool sammelt Daten über die Aktivitäten der Schüler:innen aus den digitalen Lernmitteln, die von der Schule verwendet werden. Eine potenzielle Quelle für fehlerhafte Daten ist, wenn Schüler:innen Aufgaben im Namen anderer Schüler:innen lösen, was bereits im traditionellen Bildungswesen ein Risiko ist. Durch die Verwendung eines fremden Log-ins wird ein solcher «Betrug» jedoch erleichtert. Auch die Auswirkungen können beim Einsatz von KI-Tools grösser sein, weil die Daten in ein KI-basiertes Schülerprofil einfliessen. Das System könnte bspw. fälschlicherweise annehmen, dass ein:e Schüler:in ein höheres Leistungsniveau hat, als es tatsächlich der Fall ist, und Aufgaben vorschlagen, die nicht ihren/seinen tatsächlichen Fähigkeiten entsprechen, was demotivierend sein kann. Ein ähnliches Risiko besteht, wenn ein:e Schüler:in absichtlich falsche Antworten gibt, um das System zu manipulieren und leichtere Aufgaben zu erhalten.[37]

---

35 Kritisch dazu aber: FLORENT THOUVENIN/NADJA BRAUN BINDER, Transparenz durch Datenschutzerklärungen von Behörden, ZSR 2022, 5 ff., 7 ff.

36 Siehe dazu auch “AVT – Exit report from the sandbox project with the Norwegian Association of Local and Regional Authorities (KS), the Centre for the Science of Learning & Technology (SLATE) at the University of Bergen (UiB) and the City of Oslo’s Education Agency”, 20.

37 AVT Exit Report (Fn 36), 20.

Aufgrund der Funktionsweise von KI-Tools kann es schwierig oder sogar unmöglich sein nachzuweisen, ob das personalisierte Lernmodell auf der Grundlage der richtigen Leistungen erstellt wurde und ob die für die einzelnen Schüler:innen ausgewählten Aufgaben dem tatsächlichen Lernfortschritt entsprechen. Es empfiehlt sich daher, gewisse Plausibilitätsprüfungen in ein Tool einzubauen, die bspw. bei einer bestimmten Abweichung vom Leistungsniveau der Durchschnittschüler:innen eine zusätzliche (menschliche) Überprüfung erfordern.

3.6. Datensicherheit

Verantwortliche und Auftragsbearbeiter müssen durch angemessene technische und organisatorische Massnahmen eine dem Risiko von KI-Tools entsprechende Datensicherheit gewährleisten. Ein Hauptrisiko liegt im unberechtigten Zugriff auf und in der Manipulation der Personendaten. Die zu treffenden Massnahmen richten sich nach dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem damit verbundenen Risiko.

Bei der Datensicherheit ist danach zu unterscheiden, ob ein KI-Tool auf einer **schulinternen Infrastruktur** betrieben wird oder ob Daten über Schnittstellen an ein Drittanbietersystem oder in eine Cloud übertragen werden.[38] Durch die Übertragung über eine Schnittstelle wächst zwar das Risiko einer Gefährdung der Datensicherheit, weil diese Schnittstellen bspw. dazu genutzt werden können, unbefugt auf Daten von Schüler:innen zuzugreifen. Allerdings werden **Cloud-Anbieter** in aller Regel eine höhere Datensicherheit gewährleisten können als Schulen, deren Kernkompetenzen in der Bildung und nicht im Betrieb einer IT-Infrastruktur liegt. Wenn Schulen KI-Tools einführen oder solche Tools über eine Cloud betreiben, müssen sie die notwendigen technischen und organisatorischen Massnahmen ergreifen, um die Sicherheit der Daten der Schüler:innen zu gewährleisten und entsprechende Zusagen von den Cloud-Anbietern einholen. Diese Massnahmen müssen sicherstellen, dass die Daten unbefugten Dritten nicht zugänglich sind, nicht verloren gehen und nicht unbefugt verändert werden können.

4. Auskunftsrecht

Betroffene Personen können mithilfe des Auskunftsrechts von der Schule als Verantwortliche Auskunft darüber verlangen, ob und welche Personendaten über sie bearbeitet werden. Sowohl das DSG als auch die kantonalen Datenschutzgesetze enthalten einen Katalog von Informationen, die der betroffenen Person zur Verfügung gestellt werden müssen, bspw. der Zweck der Bearbeitung, die Aufbewahrungsdauer und allfällige Empfänger von Personendaten. Die Schule bleibt auch dann auskunftspflichtig, wenn sie einen Auftragsbearbeiter einsetzt.

---

[38] Zur Festlegung der Verantwortlichkeit siehe vorne, B.2.1.

KI-Systeme sind keine strukturierten Datenbanken, die ohne weiteres nach Personendaten durchsucht werden können. Für die Verantwortlichen ist es deshalb oft kaum erkennbar, welche Daten im System konkret bearbeitet werden. Das entbindet die Schule zwar nicht von der Pflicht, einem Auskunftsbegehren nachzukommen. Die technischen Limitierungen müssen aber bei den Anforderungen an den Konkretisierungsgrad der Auskunft berücksichtigt werden. Da eine konkrete Bezeichnung der effektiv bearbeiteten Daten kaum möglich ist, wird es genügen müssen, dass die Schule in der Lage ist, über die Kategorien der bearbeiteten Daten Auskunft zu geben. Beim personalisierten Lernen können die Schüler:innen bzw. ihre Erziehungsberechtigten bspw. verlangen, dass ihnen offengelegt wird, welche Arten von Personendaten durch das KI-Tool zur Erfüllung welcher schulischen Aufgabe bearbeitet werden, wie lange die Daten gespeichert werden und an wen sie weitergegeben werden. Damit die Schule in der Lage ist, diese Auskunft zu erteilen, muss sie vor dem Einsatz eines KI-Tools sicherstellen, dass sie ein hinreichendes Verständnis von der Funktionsweise des verwendeten KI-Tools und den durch das Tool bearbeiteten und erzeugten Daten hat.

5. Durchführung einer Datenschutzfolgenabschätzung

Ist bei der Bearbeitung von Personendaten ein potenziell hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen erkennbar, muss in der Regel eine Datenschutzfolgenabschätzung (DSFA) durchgeführt werden, die die geplante Datenbearbeitung beschreibt, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen abschätzt und die Massnahmen zu deren Schutz aufzeigt. Ein hohes Risiko kann sich insb. aus dem Einsatz neuer Technologien ergeben, weshalb die Verwendung eines KI-Systems in der Regel eine DSFA erfordert. Ergibt die DSFA, dass bei der geplanten Datenbearbeitung trotz der vorgesehenen Massnahmen ein hohes Restrisiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen verbleibt, ist eine Prüfung durch den zuständigen kantonalen Datenschutzbeauftragen zwingend (sog. Vorabkontrolle).[39]

C. LEHREN UND LERNEN: USE CASE 2: LEISTUNGSBEURTEILUNG

KI-Systeme können auch für die Leistungsbeurteilung von Schüler:innen eingesetzt werden. Bei diesem Use Case werden KI-Tools behandelt, deren Beurteilung zumindest teilweise für einen **Promotionsentscheid** relevant sind. Dazu gehört auch die Entscheidung über die Aufnahme in eine Bildungseinrichtung, bspw. ein Gymnasium.

[39] Bspw. im Kanton Zürich § 10 IDG/ZH, im Kanton Fribourg Art. 42 DSchG/FR.

1. Anwendbarkeit der Datenschutzgesetze und betroffene Daten

Bei einer Leistungsbeurteilung ist es von entscheidender Bedeutung, dass die Ergebnisse, d.h. die Outputs eines KI-Tools, einer individuellen Person klar zugeordnet werden können. Um dies sicherzustellen, werden sich die Schüler:innen im KI-Tool registrieren müssen. Mit Blick auf die Vorgaben des Datenschutzrechts ist die Pseudonymisierung eine vielversprechende Option. Im vorliegenden Use Case könnten die Schüler:innen eine Prüfung unter einem Pseudonym ablegen (bspw. eine Prüfungsnummer) und nicht unter ihrem Klarnamen. Pseudonymisierte Daten sind aus Sicht der Schule jedoch weiterhin als Personendaten zu qualifizieren, weil zumindest die Schule mit einem Schlüssel die Zuordnung der Prüfungsnummern zu den einzelnen Schüler:innen vornehmen kann. Die Registrierungsdaten sind damit als Personendaten zu beurteilen.

Die Inputdaten sind je nach konkreter Ausgestaltung als Personendaten zu qualifizieren. Möglich ist auch, dass es sich um besonders schützenswerte Personendaten handelt, bspw., wenn einer Person aufgrund einer Lernschwäche mehr Zeit für die Lösung der Prüfung eingeräumt wird und dies im KI-Tool ersichtlich ist. Die Outputs, d.h. die Ergebnisse der Leistungskontrolle, sind ebenfalls Personendaten, in der Regel aber keine besonders schützenswerten Personendaten, insb. keine Gesundheitsdaten. Je nach Umfang der Leistungsbeurteilung kann jedoch ein Profiling vorliegen.[40]

2. Beteiligte und Verantwortlichkeit

Für die Beurteilung der Verantwortlichkeit kann im Wesentlichen auf die Ausführungen unter B.2.1 verwiesen werden. In der Regel wird die Schule die **Verantwortliche** sein. Der Anbieter eines KI-Tools und ein allfälliger Cloud-Anbieter dürften in der Regel als **Auftragsbearbeiter** zu qualifizieren sein.

Die Schule ist als alleinige Verantwortliche zu qualifizieren, wenn sie das KI-Tool auf einer eigenen Infrastruktur betreibt und der Anbieter des KI-Tools keine Möglichkeit hat, auf das System zuzugreifen.

Der Anbieter des KI-Tools würde hingegen zum Verantwortlichen, wenn er mit der Datenbearbeitung eigene Zwecke verfolgen würde, bspw. weil er Input- oder Outputdaten nutzt, um das eigene System weiterzuentwickeln.[41]

3. Datenbearbeitungsgrundsätze

Die Bearbeitung von Daten zur Leistungsbeurteilung kann einen signifikanten Einfluss auf das Leben der Schüler:innen haben und damit einen starken Eingriff in die Persönlichkeit darstellen. Beim Einsatz

---

40 Das Datenschutzgesetz nennt als Beispiel für ein Profiling die Analyse einer Arbeitsleistung. Ob die Analyse einer einzigen schulischen Leistung ausreicht, um ein Profiling zu begründen kann aber diskutabel sein.

41 Eine solche Datenbearbeitung wäre jedoch nur unter bestimmten Voraussetzungen möglich, siehe dazu vorne, B.2.2.

von KI-Tools zur Leistungsbeurteilung müssen deshalb die Anforderungen an die gesetzliche Grundlage, die Zweckbindung und die Verhältnismässigkeit der bearbeiteten Personendaten besonders sorgfältig abgewogen werden.[42]

Die Leistungsbeurteilung ist eine zentrale Aufgabe von Schulen, die meisten Volksschulgesetze enthalten dazu auch explizite Bestimmungen. Den Schulen kommt die Aufgabe zu, die Leistungen der Schüler:innen und ihre Lernentwicklungen regelmässig zu beurteilen. Zudem sind sie befugt, diese Leistungen zu Promotionszwecken auszuwerten (siehe bspw. § 31 Abs. 1 und § 32 Abs. 3 VSG/ZH, ähnlich Art. 37 SchG/FR). Die Gesetze enthalten in der Regel keine spezifischen Vorgaben dazu, wie die Leistungsbeurteilung vorzunehmen ist. Solange das zur Leistungsbeurteilung eingesetzte KI-Tool keine weitergehenden Datenanalysen vornimmt, als dies bei einer herkömmlichen Leistungskontrolle der Fall ist, ist eine solche **gesetzliche Grundlage** für den mit der Datenbearbeitung verfolgten Zweck ausreichend.

Nach dem Grundsatz der **Verhältnismässigkeit** dürfen nur Daten bearbeitet werden, die für das Erreichen des Bearbeitungszwecks erforderlich sind. Die Datenbearbeitung muss folglich auf die für die Leistungsbeurteilung wesentlichen Daten beschränkt bleiben. So wird es bspw. erforderlich sein, Daten über die individuelle Leistung zu analysieren, um den Lernfortschritt von Schüler:innen zu ermitteln und eine gezielte Förderung zu ermöglichen. Hingegen wird es im Rahmen der Leistungskontrolle nicht erforderlich sein, Daten zur Religion der Schüler:innen zu erfassen. Die Anmeldung und inhaltliche Zuordnung sowie automatisierte Korrekturen könnten bspw. auch über einen QR-Code erfolgen und müssen nicht über den Klarnamen laufen. Ergänzend sind Massnahmen zur **Speicherbegrenzung** zu treffen.

Da die Leistungsbeurteilung mittels KI-Tools weitreichende Folgen für die Schüler:innen haben kann, ist die **Datenrichtigkeit** besonders wichtig. Namentlich sind besondere Massnahmen zu ergreifen, dass die Daten nicht manipuliert werden können, bspw. weil Schüler:innen die Aufgaben anderer lösen. Dies betrifft auch die Gewährleistung der **Datensicherheit**. Je weitreichender der Entscheid des KI-Systems für die Promotion, desto umfassendere Anforderungen sind an die Datensicherheit zu stellen. Durch geeignete Massnahmen ist sicherzustellen, dass das System vor unbefugtem Zugriff und Manipulation geschützt ist. Dabei sind Schnittstellen so weit wie möglich zu reduzieren, um Schwachstellen zu vermeiden. Nach Möglichkeit sollten KI-Tools zur Leistungsbeurteilung für relevante Promotionsentscheide auf einer professionellen (internen) Infrastruktur, d.h. bei einem Cloud-Anbieter betrieben werden.[43]

---

42 GLASS (Fn 18), 210.

43 Siehe dazu vorne, B.3.6.

4. Besonderheiten bei automatisierten Einzelentscheidungen

Für automatisierte Einzelentscheidungen (sog. *automated decision-making*; ADM) gelten teilweise besondere Regeln, bspw. im DSG. Automatisierte Entscheidungen sind grundsätzlich zulässig, aber die betroffenen Personen müssen informiert werden, wenn ein Entscheid **ausschliesslich auf einer automatisierten Entscheidung beruht** und für sie mit einer **Rechtsfolge** verbunden ist oder sie **erheblich beeinträchtigt**. In diesem Fall besteht zudem ein Recht auf menschliches Gehör und auf menschliche Überprüfung («human in the loop»). Ergeht der Entscheid in Form einer Verfügung, liegt stets ein Entscheid mit Rechtsfolge vor. In den anderen Fällen ist zu prüfen, ob der Entscheid die betroffene Person erheblich beeinträchtigt.

Eine erhebliche Beeinträchtigung wird immer gegeben sein, wenn ein KI-System einen Promotionsentscheid fällt. In der Praxis dürften promotionsrelevante Entscheide derzeit allerdings kaum ausschliesslich auf einer automatisierten Entscheidung beruhen. In der Regel werden Lehrpersonen zumindest eine Plausibilitätsprüfung vornehmen, so dass die Regeln über ADM bei Promotionsentscheiden nicht zur Anwendung kommen. Bei anderen Leistungsbeurteilungen (bspw. einzelnen Prüfungen) sind vollständig automatisierte Entscheidungen zwar durchaus denkbar. Dort wird es aber regelmässig an der Relevanz der einzelnen Entscheidung fehlen, weshalb die besonderen Vorgaben auch hier nicht zur Anwendung kommen. Anderes dürfte allerdings gelten, wenn bspw. alle Prüfungen ausschliesslich automatisiert korrigiert werden und die Summe der Entscheide für den Übertritt in die nächste Klasse relevant ist.

Wenn ein KI-System einen Entscheid nicht alleine trifft, sondern als **Assistenz- oder Vorschlagssystem** *(decision support system)* eingesetzt wird, besteht das Risiko, dass das System faktisch wie ein automatisiertes Einzelentscheidungssystem eingesetzt wird, ohne dass es dafür konzipiert wurde. Das ist dann der Fall, wenn die Lehrpersonen die Empfehlungen des Systems in aller Regel akzeptieren, ohne eigene Überprüfungen und Bewertungen vorzunehmen, bspw. wegen einer hohen Arbeitsbelastung oder wegen mangelndem Wissen über die Funktionsweise und die Leistungsgrenzen von KI-Systemen. Es ist daher von entscheidender Bedeutung, mithilfe geeigneter Massnahmen sicherzustellen, dass die Lehrpersonen die Empfehlungen von KI-Systemen im Licht ihrer eigenen Erkenntnisse und Erfahrungen überprüfen.

5. Auskunftsrecht

Die Schüler:innen haben das Recht, Auskunft über Personendaten zu verlangen, die über sie bearbeitet werden. Leistungsanalysetools müssen deshalb so gestaltet sein, dass dieses Recht auch tatsächlich ausgeübt werden kann.

Liegt eine automatisierte Einzelentscheidung vor, besteht ein erweitertes Auskunftsrecht, das auch Informationen über die Logik der Entscheidung umfasst (bspw. Art. 25 Abs. 2 lit. f DSG). Welche

Informationen die Auskunft über die Logik umfassen muss, ist noch nicht hinreichend geklärt. Der Detaillierungsgrad der Informationen hängt zudem von der Relevanz der Entscheidung ab. Während bei einer gewöhnlichen Leistungsbeurteilung (soweit es sich dabei überhaupt um eine automatisierte Einzelentscheidung handelt) eine abstrakte Darstellung der Funktionsweise des Algorithmus ausreichen dürfte, sind bei Promotionsentscheiden, die die Zulassung zu einer Bildungseinrichtung regeln, auch weitere Angaben zu machen, etwa die dem Algorithmus vorgegebenen Ziele oder die für das Training verwendeten Datenkategorien. Auch hier sind die verschiedenen Betroffenengruppen zu berücksichtigen und je nach konkreter Schülergruppe unterschiedliche Informationen über die Logik des Systems zur Verfügung zu stellen.

6. Exkurs: Begründungspflicht

Gewisse Promotionsentscheide dürften in Form einer anfechtbaren Verfügung erlassen werden. Die öffentlich-rechtlichen Verfahrensgesetze sehen vor, dass den Adressaten einer Verfügung das Recht auf eine Begründung der Verfügung zusteht.[44] Die Begründung soll sicherstellen, dass die Betroffenen in der Lage sind, die Tragweite der Entscheidung zu beurteilen, und sie gegebenenfalls an eine höhere Instanz weiterzuziehen.[45]

KI-Systeme sind – vereinfacht ausgedrückt – darauf ausgerichtet, in den Trainingsdaten Korrelationen zu erkennen und diese auf neue Daten zu übertragen. Die Resultate sind deshalb in der Regel nicht auf Kausalitäten zurückzuführen und oft auch nicht nachvollziehbar. Dies wirft die Frage auf, ob bei Sachverhalten, in denen für einen Entscheid ein kausaler und nachvollziehbarer Grund nachgewiesen werden muss, heute überhaupt KI-Systeme eingesetzt werden können. Allerdings widmet sich die Forschungsrichtung «Explainable AI» seit einiger Zeit dem Aspekt der besseren Erklärbarkeit und Nachvollziehbarkeit von KI-basierten Entscheidungen, was erwarten lässt, dass es in Zukunft möglich sein wird, Entscheide von KI-Systemen in zutreffender und rechtlich genügender Weise zu begründen.

D. SCHULORGANISATION: USE CASE 3: STUNDENPLANGESTALTUNG

Bei diesem Use Case wird ein KI-System verwendet, um einen Stundenplan möglichst optimal zu gestalten. Das Potenzial liegt dabei nicht nur in der Zeitersparnis, sondern auch in der effizienteren Nutzung der verfügbaren Ressourcen einer Schule und der Optimierung der individualisierten Förderung von Schüler:innen.

---

44 § 10 Abs. 1 VRG/ZH; STEINMANN/SCHINDLER/WYSS, in: St. Galler Kommentar BV (Fn 19), Art. 29 N 65; BIAGGINI (Fn 19), Art. 29 N 25.

45 STEINMANN/ SCHINDLER/WYSS, in: St. Galler Kommentar BV (Fn 19); BIAGGINI (Fn 19), Art. 29 N 25; Art. 20 N 65; BGE 143 IV 40 E. 3.4.3; BGE 138 I 232 E. 5.1.

1. Anwendbarkeit der Datenschutzgesetze und betroffene Daten

Als Basisdaten werden Infrastrukturdaten (bspw. die Verfügbarkeit von Klassenzimmern oder Turnhallen) sowie Personendaten herangezogen. Die Datenbasis umfasst Informationen zu Lehr- und Assistenzpersonen, bspw. Klassenassistenzen oder Heilpädagog:innen, sowie zu Schüler:innen. Letztere umfassen persönliche Daten zu sonderpädagogischen und/oder pädagogisch-therapeutischen Massnahmen sowie die unterrichteten Fächer und Arbeitspensen.

Einige für die Stundenplanerstellung erforderliche Daten über Schüler:innen sind besonders schützenswerte Personendaten, insb. Gesundheitsdaten, bspw. Daten über Lerneinschränkungen, sonderpädagogische und/oder pädagogisch-therapeutische Massnahmen.

2. Verantwortlichkeit und Beteiligte

Bei der Verantwortlichkeit ergeben sich keine Besonderheiten. Die Schule wird für die Bearbeitung der Personendaten als Verantwortliche und der Anbieter des KI-Tools in der Regel als Auftragsbearbeiter zu qualifizieren sein. Dies gilt auch für einen etwaigen Cloudanbieter. Die Schule ist als alleinige Verantwortliche zu qualifizieren, wenn sie das KI-Tool auf ihrer eigenen Infrastruktur betreibt.

3. Datenbearbeitungsgrundsätze

Die Bearbeitung von Personendaten (insb. Daten von Lehrpersonen und Schüler:innen) durch ein KI-Tool bedarf auch bei der Stundenplangestaltung einer **gesetzlichen Grundlage**. Die relevanten Rechtsgrundlagen finden sich in den Schulgesetzen und -verordnungen. Diese schreiben den Schulen bspw. vor, bei der Gestaltung des Stundenplans die Interessen der Schüler:innen zu berücksichtigen (§ 27 VSG/ZH) und den Unterricht und die Schulfächer ausgewogen auf die Schultage zu verteilen (§ 26 VSV/ZH).

Die Bearbeitung von besonders schützenswerten Personendaten wie bspw. heilpädagogischen Massnahmen erfordert eine gesetzliche Grundlage im formellen Sinn, die den Bearbeitungszweck sowie die Art und Weise der Bearbeitung vorgibt. Im Kanton Zürich bildet § 3a VSG/ZH die allgemeine gesetzliche Grundlage, die es den Schulen erlaubt, auch besonders schützenswerte Personendaten für die Erfüllung der gesetzlich vorgesehenen Aufgaben zu bearbeiten. Diese Bestimmung dürfte für diesen Use Case ausreichen.

Der Grundsatz der **Verhältnismässigkeit** verlangt, dass nur diejenigen Daten vom KI-Tool bearbeitet werden, die für die Stundenplangestaltung erforderlich sind. Das gilt auch – und gerade – für die Bearbeitung besonders schützenswerter Personendaten. So sollten bspw. nur diejenigen Gesundheitsdaten in das KI-Tool einfliessen, die auch tatsächlich einen Einfluss auf die Stundenplangestaltung haben können. Ausserdem wäre es bei der Stundenplangestaltung möglich, die Daten über die Schüler:innen

zu aggregieren (bspw. Klasse statt individuelle Schüler:innen) oder zu pseudonymisieren. Obwohl die Schule grundsätzlich über die von allfälligen Massnahmen betroffenen Schüler:innen Bescheid weiss, kann es für die Betroffenen einen Unterschied machen, ob die Daten für alle Personen einer Schule zugänglich sind oder nur für diejenigen, die darüber Bescheid wissen müssen. Für die Personen, die mit der Stundenplangestaltung betraut sind, ist es regelmässig nicht von Relevanz, welche:r individuelle:r Schüler:in bspw. sonderpädagogische Massnahmen braucht, sondern nur, dass ein:e (oder mehrere) Schüler:in einer bestimmten Klasse durch eine heilpädagogische Fachkraft unterstützt werden sollte.

Bezüglich Datenrichtigkeit und Datensicherheit kann auf die vorstehenden Ausführungen verwiesen werden.[46]

E. SCHULORGANISATION: USE CASE 4: SCHUL- UND KLASSENZUTEILUNG

Auch im Bereich der Bildung bieten KI-gestützte Funktionen vielfältige Möglichkeiten zur Optimierung von Organisationsaufgaben, bspw. bei der Schul- und Klassenzuteilung. Durch gezielte Auswahl und Zuweisung von Schüler:innen in bestimmte Schulen oder Klassen kann ihren individuellen Bedürfnissen entsprochen werden. Bei diesem Use Case wird ein KI-System verwendet, um eine möglichst optimale Schul- und Klassenzuteilung zu erreichen.

Die **Schulzuteilung** erfolgt organisatorisch durch die Gemeinde, die zur Führung der Volksschule verpflichtet ist. Bei grösseren Gemeinden können mehrere Schulkreise gebildet werden. In diesem Fall werden die Schüler:innen zunächst einem Schulkreis zugeteilt und danach einer Schule innerhalb dieses Schulkreises. Die konkrete **Klassenzuteilung** obliegt der jeweiligen Schule. In Abhängigkeit von der Grösse einer Gemeinde kann die Entscheidung über die Klassenzuteilung bereits im Rahmen der Schulzuweisung erfolgen, bspw. wenn in einem Jahrgang lediglich eine Klasse gebildet wird.

1. Anwendbarkeit der Datenschutzgesetze und betroffene Daten

Als Basisdaten fliessen Infrastruktur- und Personendaten in das KI-System ein. Um die Schul- und Klassenzuteilung anhand einer Zielvorgabe zu steuern, werden im Rahmen der Datenbearbeitung nicht nur Adressdaten der Schüler:innen in das KI-System eingespeist, sondern auch weitere Daten, bspw. über die schulischen Leistungen, allfällige sonderpädagogische oder verstärkte Massnahmen, Daten über den sozialen und familiären Hintergrund sowie über die Muttersprache und Staatszugehörigkeit.

Bei der Zuteilung von Schulen und Klassen spielen besonders schützenswerte Personendaten oft eine entscheidende Rolle. Dies betrifft insb. Daten über sonderpädagogische Massnahmen, die als Gesund-

[46] Siehe dazu vorne, B.3.5 und B.3.6.

heitsdaten zu qualifizieren sind. Soziale und familiäre Hintergründe sowie die Muttersprache und die Staatszugehörigkeit der Schüler:innen und gegebenenfalls ihrer Familienmitglieder werden bei der Entscheidung über die Schul- oder Klassenzuteilung ebenfalls berücksichtigt. Dabei kann es sich um Daten über religiöse, weltanschauliche oder politische Ansichten oder um Daten über die Zugehörigkeit zu einer Rasse oder Ethnie handeln, die als besonders schützenswerte Personendaten gelten. Zudem ist nicht auszuschliessen, dass im Rahmen dieser Datenbearbeitung auch Daten über Massnahmen der sozialen Hilfe bearbeitet werden. Bei der Bearbeitung von Daten über schulische Leistungen über einen langen Zeitraum handelt es sich zudem um ein Profiling, für das ebenfalls besondere Anforderungen gelten.[47]

2. Verantwortlichkeit und Beteiligte

2.1. Allgemeines

Bezüglich der Verantwortlichkeit ist grundsätzlich auf das oben Gesagte zu verweisen. Eine Besonderheit besteht darin, dass bei einer **Schulzuteilung** nicht die Schule als Verantwortliche gilt, sondern die Gemeinde. Bei der Klassenzuteilung ist hingegen die zuständige Schule als Verantwortliche zu qualifizieren.

2.2. Bekanntgabe an Dritte

Die Schulzuteilung erfolgt nicht durch eine einzelne Schule, sondern je nach Grösse der Gemeinde auf Stufe der Schulgemeinde oder auf Stufe der Schulkreise innerhalb einer Schulgemeinde. Beim Umzug von Schüler:innen werden die Daten von der alten an die neue Gemeinde bzw. Schule übermittelt.

Die Bekanntgabe von Daten an andere öffentliche Organe bedarf entweder einer rechtlichen Grundlage oder kann im Einzelfall erfolgen, wenn das öffentliche Organ, das Personendaten verlangt, diese zur Erfüllung seiner gesetzlichen Aufgaben benötigt. Das VSG/ZH enthält eine Reihe von Bestimmungen, die die Bekanntgabe von Daten an andere öffentliche Organe ausdrücklich regeln, auch mit Bezug auf besonders schützenswerte Personendaten bei einem Schulwechsel (§ 3b VSG/ZH). Diese Bestimmungen dürften als Grundlage für die Bekanntgabe von Daten zur Einspeisung in ein KI-Tool genügen, das für die Schul- oder Klassenzuteilung verwendet wird.

Bezüglich der Bekanntgabe der Daten an Dritte, namentlich an die Anbieter des KI-Tools, kann auf die vorstehenden Ausführungen verwiesen werden.[48]

---

47 Siehe dazu vorne, B.3.

48 Siehe dazu vorne, B.2.2.

3. Datenbearbeitungsgrundsätze

Bei der Datenbearbeitung zur Schul- und Klassenzuteilung ist insb. zu beachten, dass die Bearbeitung von besonders schützenswerten Personendaten einer Grundlage in einem **Gesetz im formellen Sinn** bedarf. Im Kanton Zürich ist hier wiederum die allgemeine Bestimmung von § 3a VSG/ZH anzuwenden, in Verbindung mit der Aufgabenumschreibung in den anwendbaren Gesetzen und Verordnungen, bspw. der Vorschrift, dass für die Zuteilung in der Regel neben dem Wohnort weitere Personendaten wie die Sprache, die soziale Herkunft oder die Leistungsfähigkeit der Schüler:innen relevant sind (§ 25 VSV/ZH). Soweit durch die Verwendung eines KI-Tools keine weitergehenden Datenbearbeitungen vorgenommen werden als bei der «traditionellen» Zuteilung, dürften diese Bestimmungen auch für den Einsatz von KI genügen.

Der Grundsatz der **Verhältnismässigkeit** verlangt, dass nur Personendaten erhoben und bearbeitet werden, die für die Zuteilung in Schulen und Klassen tatsächlich erforderlich sind. Zur Erreichung der in den gesetzlichen Bestimmungen genannten Ziele können verschiedene Daten berücksichtigt werden, bspw. Wohnsitz, Leistungsfähigkeit, soziale und sprachliche Herkunft und Verteilung der Geschlechter.[49] Der Einbezug von zusätzlichen vorhandenen Daten wäre denkbar, wenn dies zu einem besseren Ergebnis bei der Zuteilung führen könnte. In diesem Fall wäre eine Interessensabwägung durchzuführen.

Besondere Sorgfalt ist bei der Gewährleistung der **Datenrichtigkeit** aufzuwenden. Eine Vielzahl der bearbeiteten Daten kann sich ändern, bspw. die Anzahl der Geschwister oder der Zivilstand der Eltern. Bei Kriterien, die für die Zuteilung relevant sind, ist durch geeignete Massnahmen sicherzustellen, dass die verwendeten Daten aktuell und richtig sind.

Wichtig sind auch angemessene Massnahmen zur **Datensicherheit**, namentlich wenn besonders schützenswerte Personendaten bearbeitet werden.[50]

4. Besondere Vorgaben bei automatisierten Einzelentscheidungen

Ergänzend können die Vorgaben zu den automatisierten Einzelentscheidungen Anwendung finden. Im vorliegenden Use Case werden KI-Tools eingesetzt, um Schüler:innen gestützt auf die vordefinierten Basisdaten zu Schulen oder Klassen zuzuteilen. Erfolgt der Entscheid vollständig durch das KI-Tool, liegt eine automatisierte Einzelentscheidung vor, zumal Schul- und Klassenzuteilungen die nötige Relevanz haben dürften, um als automatisierte Einzelentscheidungen zu gelten.[51]

---

49 Siehe bspw. § 25 Abs. 1 Volksschulverordnung des Kantons Zürich.

50 Siehe dazu vorne, B.3.6.

51 Zur Relevanz siehe vorne, C.4.

In der Praxis dürfte es jedoch selten vorkommen, dass ein KI-Tool allein über die Schul- und Klassenzuteilung entscheidet. Vielmehr werden die Tools als Assistenztools Empfehlungen oder Vorschläge abgeben, die danach von Menschen zumindest auf ihre Plausibilität überprüft werden. Dabei ist darauf zu achten, dass eine «menschliche Überprüfung» auch tatsächlich stattfindet.[52]

5. Auskunftsrecht

Die Betroffenen haben das Recht, Auskunft darüber zu erhalten, welche Daten über sie gespeichert und wie diese bearbeitet werden. Die Schulen müssen sicherstellen, dass sie die Auskunft gegenüber allen Betroffenen gewährleisten können. Liegt eine automatisierte Einzelentscheidung vor, ist bei der Geltendmachung des Auskunftsrechts auch über die involvierte Logik zu informieren.

6. Exkurs: Begründungspflicht

Entscheidungen über Schul- und Klassenzuteilungen gelten in gewissen Kantonen als anfechtbare Verfügungen.[53] Im Kanton Zug werden Entscheide über die Zuteilung in eine Parallelklasse an der gleichen Schule, die Eröffnung und Schliessung von Klassen sowie die Zuteilung von Klassen zu bestimmten Schulhäusern hingegen als nicht anfechtbare schulorganisatorische Massnahmen verstanden.[54] Bei Verfügungen haben die Betroffenen das Recht auf eine Begründung. Dies wirft die Frage auf, ob die Outputs eines KI-Systems überhaupt begründbar sind. Auch hier dürften die Entwicklungen im Bereich Explainable AI von Bedeutung sein. Diese dürften es in Zukunft möglich machen, Entscheidungen von KI-Systemen in zutreffender und rechtlich genügender Weise zu begründen.

---

52 Zu den «faktischen» ADM siehe vorne, C.4.

53 Siehe dazu Verwaltungsgericht ZH, VB.2015.00551, vom 11. Mai 2015.

54 «https://www.zg.ch/behoerden/direktion-fur-bildung-und-kultur/schulinfo/schule/verfuegungen-im-schulbereich».