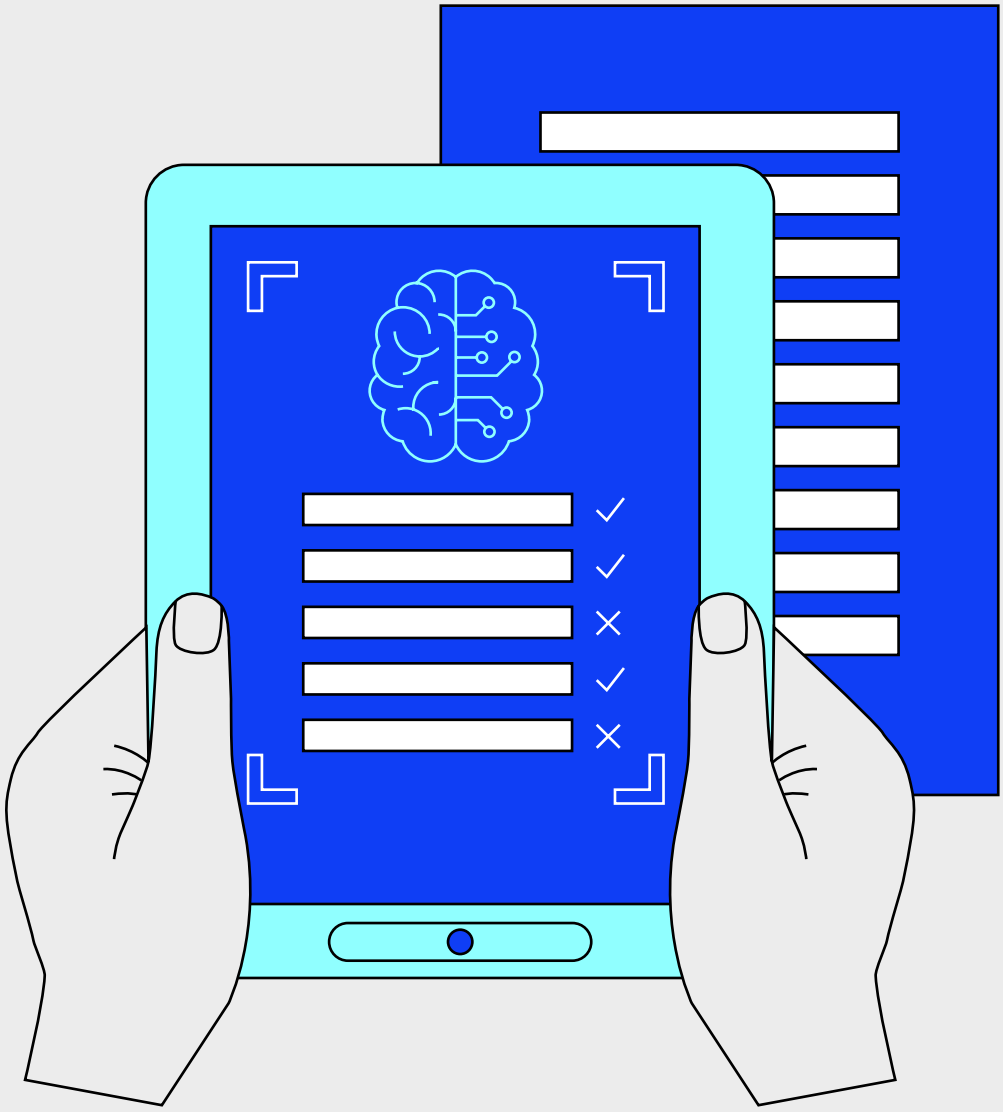
Innovation-Sandbox
für Künstliche Intelligenz



Künstliche Intelligenz in der Bildung

Rechtliche Best Practices

metropolitan konferenz zürich

Kanton Zürich

Innovation Zurich

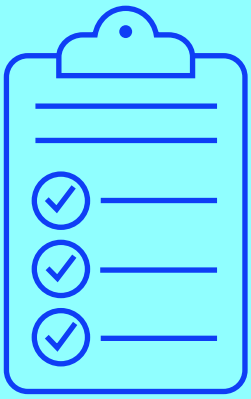
Künstliche Intelligenz (KI) bietet in der Bildung Potenzial für individualisiertes Lernen und unterstützt Lehrkräfte bei repetitiven Aufgaben wie Korrekturen. Es gibt jedoch regulatorische und ethische Herausforderungen. Eine Vielzahl KI-unterstützter Tools ist bereits in Schulen im Einsatz. Oftmals sind den Lösungsanbietern, Lehrpersonen oder Schulverantwortlichen die rechtlichen Rahmenbedingungen in Bereichen wie Datenschutz und Urheberrecht unklar. Dieser Leitfaden bietet einen Überblick über rechtliche Aspekte bei der Implementierung von KI-Anwendungen. Das Dokument wurde basierend auf einem konkreten Anwendungsfall erarbeitet, bei dem Schüler:innen mit einem Smartphone-Scan handschriftlich ausgefüllte Aufgaben automatisiert korrigierten. Die nachfolgenden Ausführungen basieren auf den Rechtsgrundlagen einer öffentlichen Schule im Kanton Zürich. Die Rechtslage in anderen Kantonen ist vergleichbar, die Bestimmungen werden allerdings unterschiedlich angewendet. Der Leitfaden richtet sich vor allem an Anbieter, kann aber auch Schulverantwortlichen aufschlussreiche Erkenntnisse bieten.

Innovation-Sandbox für KI

Das vorliegende Dokument wurde im Rahmen der Innovation-Sandbox für KI erarbeitet. Die Sandbox ist eine Testumgebung für die Umsetzung von KI-Projekten aus verschiedenen Sektoren. Die breit abgestützte Initiative aus Verwaltung, Wirtschaft und Forschung soll verantwortungsvolle Innovation fördern, indem das Projektteam und teilnehmende Organisationen eng mit regulatorischen Fragestellungen arbeiten und die Nutzung von neuartigen Datenquellen ermöglichen.
Mehr Informationen

I.

Vorbereitung eines KI-Projekts



1. Ermittlung der betroffenen Rechtsgebiete

Aus rechtlicher Sicht geht es in einem ersten Schritt darum, die betroffenen Rechtsgebiete zu ermitteln. **Datenschutzrecht** dürfte in den allermeisten Fällen eine grosse Rolle spielen, jedoch können je nach konkreter Anwendung auch andere Rechtsgebiete relevant werden, bspw. das **Urheberrecht,** Teile des **Verwaltungsrechts (insbesondere das Schulrecht)** oder auch das allgemeine **Vertragsrecht,** wenn es um die Gestaltung der Beziehung zwischen dem Anbieter des KI-Tools und der Schule geht.

Die Ermittlung der betroffenen Rechtsgebiete erfolgt im Idealfall durch den Anbieter des KI-Tools und die vonseiten der Schule involvierten Personen gemeinsam. Für die Beteiligten kann es sich auch lohnen, sich an eine kantonale Stelle zu wenden, etwa an die Bildungsdirektion, die für Digitalisierungsthemen zuständig ist.

2. Ermittlung der einschlägigen Rechtsgrundlagen

Wenn die betroffenen Rechtsgebiete feststehen, ist in einem nächsten Schritt zu eruieren, welche Rechtsgrundlagen Anwendung finden. Gerade im Bereich des Datenschutzes ist die Ermittlung der anwendbaren Rechtsgrundlagen nicht immer einfach. Die Datenbearbeitung durch Private und durch Bundesbehörden unterliegt dem **Bundesgesetz über den Datenschutz (DSG)**, wobei innerhalb des Gesetzes unterschiedliche Vorschriften für verschiedene Instanzen zur Anwendung kommen. Der private Anbieter eines KI-Tools hat für seine eigene Datenbearbeitung die einschlägigen Vorschriften des DSG zu beachten. Dasselbe gilt, wenn er das KI-Tool Privaten oder einer Bundesbehörde anbietet.

Volksschulen sind kantonale öffentliche Organe. Auf kantonale und kommunale Datenbearbeitungen kommen die kantonalen Vorschriften zur Anwendung, im Kanton Zürich ist dies das **Gesetz über die Information und den Datenschutz (IDG)**. Die Schulen im Kanton Zürich müssen sich an das IDG halten. Ergänzend gelten kommunale Erlasse wie Gemeindegesetze oder bildungsspezifische Erlasse wie das Volksschulgesetz. In manchen Schulen oder Bildungseinrichtungen gibt es auch interne Richtlinien, die beachtet werden müssen. Die Schulen haben dafür zu sorgen, dass auch Dritte, die sie zur Erfüllung ihrer öffentlichen Aufgaben hinzuziehen, die für sie geltenden Vorschriften einhalten. Für die Anbieter bedeutet dies, dass sie in der Lage sein müssen, die teilweise strengen Vorgaben einzuhalten, die für die Datenbearbeitungen durch eine öffentliche Institution gelten. Beispielsweise können für ein Gemeinwesen besondere Regeln für die Nutzung von Cloud-Diensten gelten.

«KI-Projekte an Schulen sind aus rechtlicher Sicht vielschichtig, weshalb sich eine holistische Herangehensweise empfiehlt.»

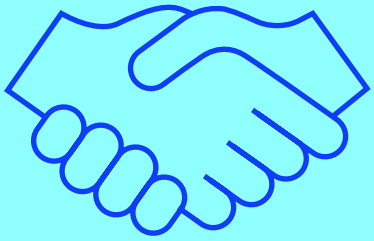
Stephanie Volz, ITSL Universität Zürich

3. Miteinbezug der betroffenen Institutionen

Wer als Anbieter eines KI-Tools mit einer Schule zusammenarbeiten möchte, sucht oft den Kontakt zu einer Lehrperson. Obschon die Lehrperson quasi der Schlüssel zum Klassenzimmer ist, sollte der Einbezug von weiteren Personen und Institutionen nicht vergessen werden. Mögliche Personen bzw. Stellen sind die Schulleitung oder die ICT- oder Digitalisierungsverantwortliche in Schulen. Je nach Grösse und Risiko des Projekts ist es sinnvoll, sich als Erstes an die zuständige Bildungsdirektion zu wenden. Je nach Vorhaben ist es auch empfehlenswert, die kantonalen Datenschutzbehörden gleich zu Beginn des Projekts einzubeziehen, weil in den meisten Kantonen eine sog. Vorabkontrolle (dazu III.6) des Projekts durch die Datenschutzbehörden erforderlich sein dürfte. Durch die Involvierung verschiedener Stellen kann das Projekt breit abgestützt und mögliche Probleme bereits frühzeitig erkannt und adressiert werden. Diese Faktoren sind massgebend, damit ein Projekt zum Erfolg werden kann.

II.

Durchführung des Projekts



1. Klärung von Haftung und Verantwortung

Weitere wichtige Punkte, die zwischen den Beteiligten zu klären sind, sind die Verantwortung und die Haftung. Dazu sind in einem ersten Schritt die Kompetenzen zu klären («Wer darf überhaupt was?»), gestützt darauf sind die Rollen zu definieren und die Aufgaben bzw. die Rechte und Pflichten zu verteilen. Die Beteiligten sollten sich Gedanken machen, wie sich allfällige Risiken am besten minimieren lassen.

Wesentlich ist die Klärung der datenschutzrechtlichen Verantwortung bzw. die Auferlegung der datenschutzrechtlichen Pflichten (vgl. dazu III.2.). Damit verbunden ist auch die Klärung von allfälligen Haftungsfragen für den Fall, dass es zu einem Schaden kommt. Aus datenschutzrechtlicher Sicht ergibt sich die Haftungssituation oft aus den kantonalen Bestimmungen. Die Schule als öffentliches Organ bleibt in der Regel verantwortlich, auch wenn Dritte eine Datenbearbeitung vornehmen. Sie wird den Anbietern des KI-Tools jedoch vertraglich gewisse Pflichten auferlegen (müssen), die bei der Bearbeitung von Personendaten zu beachten sind. Anbieter, die diese Pflichten nicht einhalten, werden gegenüber dem Gemeinwesen haftbar.

2. Identifizierung der rechtlichen Grundlagen

Die Bearbeitung von Personendaten durch ein öffentliches Organ wie die Schule ist nur zulässig, wenn eine rechtliche Grundlage vorhanden ist **(Grundsatz der Rechtmässigkeit)**. Der wichtigste Schritt vor einer Datenbearbeitung durch eine Schule ist deshalb, die anwendbare rechtliche Grundlage zu identifizieren. Diese findet sich in der Regel im Recht der jeweiligen Bereiche, für die Schule in den einschlägigen Volksschulgesetzen oder in darauf abgestützten Erlassen. Eine rechtliche Grundlage kann ein Gesetz oder eine Verordnung sein.

> «Geklärte Rahmenbedingungen sind eine notwendige Voraussetzung für einen vertrauensvollen Einsatz von KI in der Bildung.»
>
> Nelly Buchser, Educa

Die meisten Volksschulgesetze enthalten rechtliche Grundlagen für eine Reihe von Datenbearbeitungen. Auch die Schulkreise oder die einzelnen Schulen können über gewisse Rechtsgrundlagen verfügen. Welche einschlägig sind und ob diese im konkreten Fall auch für die Nutzung von KI-Tools ausreichen, ist im Einzelfall zu klären. In vielen Fällen dürften die gesetzlichen Grundlagen, welche die Datenbearbeitung zur Erfüllung des Bildungsauftrags abdecken, auch den Einsatz von KI-Tools umfassen.

III.

Datenschutz-rechtliche Implikationen

1. Umgang mit Personendaten

Die (eidgenössischen oder kantonalen) Datenschutzgesetze kommen dann zur Anwendung, wenn Personendaten bearbeitet werden. **Personendaten** sind alle Angaben, die sich auf eine **bestimmte oder bestimmbare Person** beziehen. Die Person ist bestimmbar, wenn sich ihre Identität direkt aus den Daten selbst oder aus dem Kontext in Kombination mit weiteren Daten ergibt, soweit es zur Feststellung der Identität keines unverhältnismässigen Aufwands bedarf. Die Bestimmbarkeit ist relativ, d.h., eine Person kann für eine Person mit Zusatzwissen identifizierbar sein, für eine andere nicht.

Nimmt man handschriftlich erfasste Daten als Beispiel, wären handschriftlich ausgefüllte Arbeitsblätter für Lehrpersonen häufig als Personendaten zu qualifizieren, weil die Lehrperson in der Regel in der Lage ist, anhand der Handschrift ihre Schüler:innen zu identifizieren. Ob für den Anbieter eines KI-Tools auch Personendaten vorliegen, ist im Einzelfall zu klären: Wenn der KI-Anbieter nur die handschriftlich ausgefüllten Arbeitsblätter ohne weitere identifizierende Merkmale (bspw. den Namen), aus denen er einen Bezug zu einer Person herstellen könnte, erhält, handelt es sich nicht um Personendaten. Wenn ein Arbeitsblatt identifizierbare Merkmale enthält, bspw. weil es mit dem Namen beschriftet ist, liegen Personendaten vor. Wenn Personendaten vorliegen, kommen die einschlägigen Datenschutzgesetze zur Anwendung, und die Bearbeitung hat den darin festgelegten Anforderungen zu entsprechen. Ziel bei der Entwicklung eines KI-Tools sollte also sein, dass erst gar keine oder so wenig Personendaten wie möglich entstehen. Weil bereits wenige Anhaltspunkte genügen, dass ein Bezug zu einer bestimmten Person hergestellt werden kann, ist die Entstehung von Personendaten allerdings oft nicht zu vermeiden.

2. Klärung der datenschutzrechtlichen Verhältnisse

Eine aus datenschutzrechtlicher Sicht grundlegende Frage ist diejenige der datenschutzrechtlichen Verantwortlichkeit. Verantwortlich ist, wer – allein oder zusammen mit anderen – über den Zweck und die Mittel einer Datenbearbeitung entscheidet. Diese Person ist grundsätzlich für die Einhaltung des Datenschutzes verantwortlich.

Wenn eine staatliche Schule zur Erfüllung ihrer Aufgaben KI-Tools einsetzt und dabei Personendaten bearbeitet werden, ist diese Konstellation aus datenschutzrechtlicher Sicht als Auslagerung bzw. als Auftragsdatenbearbeitung zu qualifizieren. Die Datenbearbeitung der Schule wird zusammen mit einem oder durch einen Dritten wahrgenommen. Die Schule bleibt allerdings für die Bearbeitung verantwortlich. Darum ist für die Datenbearbeitenden auch das gleiche Recht anwendbar wie für das öffentliche Organ, das die Datenbearbeitung ausgelagert hat. Bei öffentlich-rechtlichen Schulen gilt im Kanton Zürich das IDG und bei privaten Schulen das DSG.

Das öffentliche Organ muss seine Verantwortung auf verschiedene Arten wahrnehmen. Eine davon ist die vertragliche Einbindung der Dritten in die Verantwortung. Das geschieht durch Abschluss eines Vertrags, der von Gesetzes wegen bestimmte Mindestinhalte aufweisen muss. Im Kanton Zürich finden sich die einschlägigen Bestimmungen bspw.

in der Verordnung über die Information und den Datenschutz. Diese finden sich abgebildet in den AGB des Regierungsrats zu Informatikleistungen. Es können aber auch individuell gleichwertige Bestimmungen ausgehandelt werden.

3. Beachtung der relevanten Datenschutzgrundsätze

Datenschutz ist eines der wichtigsten Themen bei der Implementierung von digitalen Lösungen in Schulen. Damit ein Projekt datenschutzkonform ist, müssen die Datenschutzgrundsätze eingehalten werden. Die Einhaltung der Datenschutzgrundsätze ist in jedem Stadium eines Projekts zu gewährleisten. Wichtig ist, die Grundsätze bereits bei der Entwicklung eines Produkts zu implementieren (Privacy by Design). Zudem sind allfällige Voreinstellungen möglichst datenschutzfreundlich, d.h. so, dass möglichst wenig Daten bearbeitet werden, zu gestalten (Privacy by Default). Die Datenschutzgrundsätze finden sich in ähnlicher Form im DSG wie auch in den kantonalen Datenschutzgesetzen.

Neben dem bereits erwähnten Grundsatz der Rechtmässigkeit bzw. der Gesetzesmässigkeit, der bei der Datenbearbeitung durch staatliche Stellen

«Das Anfallen von Personendaten, die für eine KI-Anwendung nicht zwingend benötigt werden, erhöht die rechtliche Komplexität massiv.»

Stephanie Volz, ITSL Universität Zürich

wie die Schule eine rechtliche Grundlage verlangt (vgl. dazu II.2.), gibt es eine Reihe von weiteren Grundsätzen, die eingehalten werden müssen.

Wesentlich ist der Grundsatz der Verhältnismässigkeit. Die Datenbearbeitung muss geeignet und erforderlich sein, um den gewünschten Zweck zu erreichen, d.h., Datenbearbeitungen sind auf das erforderliche Minimum zu beschränken. So ist bspw. die Angabe des genauen Geburtsdatums bei der Registrierung für das KI-Tool in der Regel nicht notwendig. Auch die Nutzung eines Tools ohne vorgängige Registrierung (ein sog. Gastzugang) dient der Gewährleistung der Verhältnismässigkeit. Die Anmeldung wie auch die Zuordnung der Lerninhalte und automatisierte Korrekturen könnten bspw. durch einen QR-Code erfolgen. Ergänzt wird der Grundsatz durch das Prinzip der Datenminimierung, wonach Personendaten, die für den Bearbeitungszweck nicht mehr notwendig sind, vernichtet oder anonymisiert werden. Dies bedeutet auch, dass die Daten sowohl bei der Lehrperson als auch beim Anbieter des KI-Tools nur so lange gespeichert werden dürfen, wie dies notwendig ist.

Nach dem Grundsatz der Zweckbindung dürfen Daten nur zu dem Zweck bearbeitet werden, zu dem sie erhoben worden sind. Dieser Zweck muss für die betroffene Person erkennbar sein. Nicht nur der Zweck, auch die Datenbearbeitung an sich muss erkennbar sein. Bei der Bearbeitung durch ein Gemeinwesen ergibt sich die Transparenz oft aus der gesetzlichen Grundlage (Grundsatz der Transparenz). Zur Gewährleistung der Transparenz enthalten die Datenschutzgesetze mehr oder weniger umfangreiche Informationspflichten für die Bearbeiter von Personendaten.

Wenn ein Datenbearbeitungsgrundsatz verletzt ist, führt dies zur Unrechtmässigkeit der Datenbearbeitung. Damit die Datenbearbeitung durchgeführt werden darf, ist ein Rechtfertigungsgrund erforderlich.

4. Einhaltung der Informationspflichten

Das DSG wie auch kantonale Datenbearbeitungsgesetze wie das IDG verpflichten die Verantwortlichen, d.h. die Schulen, die betroffenen Personen über die Datenbearbeitungen zu informieren. Das DSG verlangt, dass mindestens die Identität und die Kontaktdaten der bearbeitenden Stelle, der Bearbeitungszweck und allfällige Empfänger oder die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden, mitgeteilt werden. Gemäss IDG ist zusätzlich über die beschafften Daten und über die Rechtsgrundlage der Bearbeitung zu informieren. Obwohl die Einhaltung der Informationspflichten den Schulen als Verantwortlichen obliegt, werden die Anbieter des KI-Tools bei der

konkreten Umsetzung in der Regel mitwirken müssen.

5. Sicherstellung der Daten- und Informationssicherheit

Ein grosses Risiko für Personendaten liegt in der Regel in einem unerlaubten Zugriff auf Daten. Aus diesem Grund sind Verantwortliche dazu verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzgrundsätze eingehalten werden, und durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten. Die zu ergreifenden Massnahmen richten sich nach dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem mit der Bearbeitung verbundenen Risiko.

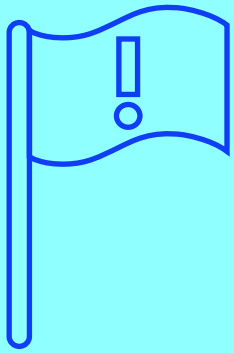
Bei der Gestaltung eines KI-Tools ist darauf zu achten, dass so wenig Personendaten wie möglich anfallen, bspw. durch die Vermeidung der Nutzung von Personendaten beim Anmeldeprozess (vgl. dazu III.3.). Ein weiteres Beispiel: Damit sichergestellt werden kann, dass die Schüler:innen nicht statt der Arbeitsblätter aus Versehen persönliche Dokumente wie Bankauszüge oder Gesundheitsakten hochladen, kann durch technische Vorkehrungen sichergestellt werden, dass ein Upload nur möglich ist, wenn ein Arbeitsblatt erkannt wird.

6. Durchführung einer Datenschutz-Folgenabschätzung

Im Kanton Zürich müssen öffentliche Organe und damit auch die Schulen vor einer beabsichtigten neuen Datenbearbeitung eine **Datenschutz-Folgenabschätzung (DSFA)** vornehmen, welche die Risiken für die Einhaltung der Grundrechte der betroffenen Personen beurteilt. Die Umsetzung von Digitalisierungsprojekten und der Einsatz von neuen Technologien sind neue Datenbearbeitungen und bedürfen einer vorgängigen DSFA. Ergeben sich aus der DSFA besondere Risiken für die Einhaltung der Grundrechte der betroffenen Personen, ist die beabsichtigte Bearbeitung von Personendaten vorab den kantonalen Datenschutzbeauftragten zur Prüfung zu unterbreiten (Vorabkontrolle). Projekte mit Einsatz von KI arbeiten mit neuen Technologien, die besondere Risiken für die Grundrechte der betroffenen Personen beinhalten und in jedem Fall den Datenschutzbeauftragten zur Vorabkontrolle eingereicht werden müssen. Im Rahmen der **Vorabkontrolle** prüfen die Datenschutzbeauftragten, ob das entsprechende Vorhaben datenschutzkonform umgesetzt werden kann oder ob Anpassungen vorgenommen werden müssen. Für die Vorabkontrolle sind den Datenschutzbeauftragten verschiedene Dokumente einzureichen. Dazu gehören ein ISDS-Konzept, die DSFA und die Rechtsgrundlagenanalyse. Das Einreichen der DSFA obliegt der Schule. Damit die DSFA korrekt vorgenommen werden kann, müssen die Anbieter der Schule jedoch gewisse Informationen über das angebotene KI-Tool zur Verfügung stellen.

IV.

Punkte von besonderem Interesse



1. Vorsicht bei der Bearbeitung von Personendaten von Kindern

Wenn KI-Tools in der Schule eingesetzt werden, geht es in der Regel um die Bearbeitung von Daten, die Kinder betreffen (Lernerfolg usw.). Dennoch ist auf das besondere Risiko bei der Datenbearbeitung Rücksicht zu nehmen, bspw. im Rahmen der DSFA (vgl. dazu III.6.).

Auch bei der Prüfung, ob dem Grundsatz der Verhältnismässigkeit Rechnung getragen wurde, sind die besonderen Umstände, die bei der Bearbeitung von Daten von Kindern vorliegen, zu beachten. Des Weiteren müssen Informations- und Transparenzpflichten gegenüber Kindern auch gegenüber den Eltern wahrgenommen werden, was bedeutet, dass die Erziehungsberechtigten über allfällige Datenbearbeitungen zu informieren sind. Wenn eine Datenbearbeitung eine Einwilligung erfordert, so ist die Einwilligung der Erziehungsberechtigten einzuholen (vgl. dazu IV.5.). Diese Pflichten obliegen in der Regel der Schule, die Anbieter werden der Schule jedoch gewisse Informationen zur Verfügung stellen müssen.

2. Vorsicht bei der Bearbeitung von besonders schützenswerten Personendaten oder Profilings

Sowohl das eidgenössische wie auch die kantonalen Datenschutzgesetze unterscheiden zwei Kategorien von Personendaten. Neben den «normalen» Personendaten gibt es sogenannte besonders schützenswerte oder «besondere» Personendaten, deren Bearbeitung an besondere Voraussetzungen geknüpft ist.

Als besonders schützenswerte Personendaten gelten nach Bundesrecht (und in ähnlicher Form im kantonalen Recht) Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten, die eine natürliche Person eindeutig identifizieren, Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen sowie Daten über Massnahmen der sozialen Hilfe. Im Bereich der Schule kann es vorkommen, dass besonders schützenswerte Personendaten bearbeitet werden, infrage kommen insbesondere Gesundheitsdaten (bspw. schulrelevante Diagnosen wie Hinweise auf Legasthenie oder Dyskalkulie), Angaben über die Religion oder im Einzelfall biometrische Daten. Wichtig ist im Zusammenhang mit biometrischen Daten, dass diese nur dann als besonders schützenswerte Daten gelten, wenn es sich um durch ein spezifisches technisches Verfahren gewonnene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums handelt, die eine eindeutige Identifizierung der betroffenen Person ermöglichen oder eine bestehende Identifizierung bestätigen. KI-Tools können bspw. dann biometrische Daten bearbeiten, wenn sie auf einer technischen Analyse von Handschriften oder Stimmerkennung beruhen.

Besondere Vorschriften bestehen auch dann, wenn Informationen in einer Form zusammengestellt werden, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben. Man spricht in diesem Zusammenhang von Persönlichkeitsprofilen oder Profilings, die ebenfalls besondere Personendaten darstellen.

Die Bearbeitung von besonders schützenswerten Personendaten bzw. das Profiling bedarf einer Grundlage in einem Gesetz im formellen Sinn, d.h., das Gesetz muss durch das zuständige Parlament – Kantons- oder Gemeinderat – beschlossen worden sein. Das zürcherische Volksschulgesetz, in dem sich verschiedene gesetzliche Grundlagen für schulische Datenbearbeitungen finden, gilt als Gesetz im formellen Sinn, entsprechend kann es in gewissen Fällen als Grundlage für die Bearbeitung von besonders schützenswerten Personendaten dienen, wenn es eine hinreichend bestimmte Regelung für entsprechende Datenbearbeitungen enthält.

3. Vorsicht bei der Verwendung von (Personen-)Daten für eigene Zwecke

Anbieter von KI-Tools haben oft ein Interesse daran, die bei der Verwendung anfallenden Daten für eigene Zwecke zu nutzen. So können die Daten aus den Korrekturen bspw. nützlich sein, um das KI-Tool weiter zu trainieren oder die Dienstleistung weiterzuentwickeln.

Wenn die Daten in der Schule in anonymisierter Form anfallen und entsprechend keine Personendaten mehr vorliegen, ist eine Weitergabe dieser Daten aus Sicht des Datenschutzes ohne Weiteres zulässig. Die Anonymisierung von (Personen-)Daten ist jedoch als eigene Datenbearbeitung zu qualifizieren.

Wenn die (Personen-)Daten, die in der Schule erhoben werden, zu einem anderen Zweck als zu dem ursprünglich erhobenen bearbeitet werden sollen, liegt aus datenschutzrechtlicher Sicht eine Zweckänderung vor, und eine solche bedarf einer rechtlichen Grundlage. Dies bedeutet, dass es für die Verwendung der Korrekturdaten für Trainings- und Weiterentwicklungszwecke der KI eine eigene gesetzliche Grundlage bräuchte, die in der Regel nicht vorhanden ist.

Um die Daten trotzdem nutzen zu können, bestehen im Kanton Zürich theoretisch zwei Möglichkeiten: Die Bekanntgabe von Personendaten an Dritte ist zulässig, wenn **im Einzelfall eine Einwilligung** vorliegt. Damit Personendaten von Schüler:innen bekannt gegeben werden dürfen, müssten die Einwilligungen der betroffenen Schüler:innen bzw. ihrer Erziehungsberechtigten vorliegen. Ob und in welchem Umfang diese Bestimmung im konkreten Fall zur Anwendung kommen kann, ist im jeweiligen Einzelfall zu klären.

Eine weitere Möglichkeit besteht, wenn eine **nicht personenbezogene Datenbearbeitung** vorliegt. Die meisten Datenschutzgesetze sehen die Möglichkeit vor, dass staatliche Stellen Daten zu nicht personenbezogenen Zwecken bekannt geben dürfen, bspw. Daten zu Forschung, Planung oder Statistik. Voraussetzung ist, dass die Daten vorgängig anonymisiert worden sind und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind. Das Training und die Weiterentwicklung von KI-Tools kommen als nicht personenbezogene Zwecke infrage. Auch bei dieser Variante ist im Vorfeld zu klären, ob sie im konkreten Einzelfall angerufen werden kann, weil die Auslegung der Bestimmungen in den Kantonen sehr unterschiedlich ist.

Neben den datenschutzrechtlichen können sich auch urheberrechtliche Probleme stellen. Bislang ungeklärt ist, ob die Nutzung von urheberrechtlich geschützten Werken zum Trainieren von KI eine urheberrechtlich relevante Handlung darstellt, und wenn ja, ob die Berufung auf die Data-Mining-Ausnahme von Art. 24d URG (Urheberrechtsgesetz) infrage kommt. Diese Bestimmung erklärt die Bearbeitung von urheberrechtlich geschützten Werken zu wissenschaftlicher Forschung unter gewissen Voraussetzungen als zulässig. Die Bestimmung gilt grundsätzlich auch für kommerzielle Zwecke und könnte entsprechend auch für das Trainieren von KI-Tools zur Anwendung kommen. Die Rechtslage ist jedoch umstritten, weshalb eine vertiefte juristische Abklärung im Einzelfall angezeigt ist.

4. Vorsicht bei der Verwendung von Lehrmitteln?

Wenn ein KI-Tool Fotos, Texte o.Ä. von bestehenden Lehrmitteln verwendet, ist zusätzlich das Urheberrecht zu beachten. Die Digitalisierung von Lehrmitteln ist als urheberrechtlich relevante Vervielfältigungshandlung zu qualifizieren, was grundsätzlich der Zustimmung des Urhebers bedarf. Das schweizerische Urheberrecht kennt zwar die Schranke der Verwendung von urheberrechtlich geschützten Werken im Unterricht, deren Anwendbarkeit beschränkt sich jedoch auf die Verwendung der Werke im Unter-

richt selbst. Die kommerzielle Verwertung der Werke ist davon nicht betroffen. Der Anbieter des KI-Tools verfolgt in der Regel eigene kommerzielle Zwecke, weshalb die Schranke keine Anwendung finden dürfte. Wenn der Anbieter eines KI-Tools bestehende Lehrmittel nutzen möchte, wäre das Einverständnis des Urhebers einzuholen.

5. Vorsicht bei der Einbindung von Large Language Models

Anbieter von KI-Tools haben die Möglichkeit, Large Language Models (LLM) über eine Schnittstelle (API) in das eigene KI-Tool einzubinden. Bei der Einbindung solcher Dritt-Tools ist jedoch aus rechtlicher Sicht Vorsicht geboten. Bezüglich des Datenschutzrechts ist darauf zu achten, dass keine Personendaten an den LLM-Anbieter fliessen und möglichst auch nicht unabsichtlich fliessen können. Auch dem Thema Datensicherheit ist Rechnung zu tragen. Zudem kann es zu urheberrechtlichen Problemen kommen, wenn der LLM-Anbieter urheberrechtlich geschützte Inhalte widerrechtlich für sein Modell verwendet und diese rechtsverletzenden Inhalte im KI-Tool auftauchen.

«Die Einbindung von Large Language Models bringt für Hersteller Grosse Chancen, führt aber auch zu rechtlichen Risiken, die schwierig zu kontrollieren sind.»

Raphael von Thiessen, Leiter Innovation-Sandbox für KI

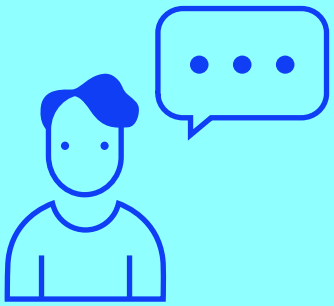
6. Wenig relevant: Einwilligung

Eine Datenbearbeitung bedarf in wenigen Fällen einer Einwilligung. Eine Einwilligung kann im Einzelfall dazu dienen, eine ansonsten unzulässige Datenbearbeitung zu rechtfertigen. In gewissen Fällen können staatliche Organe, wenn keine (genügende) gesetzliche Grundlage vorliegt bzw. die Daten zu einem anderen Zweck verwendet werden sollen als dem ursprünglich erhobenen, von den Betroffenen eine Einwilligung einholen. Das Einholen einer solchen Einwilligung ist jedoch auf den Einzelfall beschränkt. Bei Privaten gelten neben der Einwilligung auch überwiegende private oder öffentliche Interessen als Rechtfertigungsgrund. Dazu zählt auch die nicht personenbezogene Bearbeitung zum Zweck der Forschung. Dieser Grund könnte bspw. bei der Nutzung von Daten zum Trainieren und Testen des KI-Tools zur Anwendung kommen. Die Rechtslage ist jedoch in dieser Hinsicht umstritten.

Die Einholung der Einwilligung dürfte somit nur in den wenigsten Fällen notwendig sein. Weil das Einholen einer Einwilligung zudem an diverse Voraussetzungen geknüpft ist, bspw. die Freiwilligkeit, die das Vorliegen einer echten Wahl verlangt, ist die Einwilligung als Grundlage für eine Datenbearbeitung oft nicht empfehlenswert.

V.

Empfehlungen des Sandbox-Teams



Die rasante Entwicklung von KI im Bildungsbereich bringt erhebliche Potenziale, jedoch auch grosse Herausforderungen, besonders im rechtlichen und ethischen Bereich. Es besteht eine dringende Notwendigkeit für klare Richtlinien und einen intensiven interdisziplinären Dialog, um sicherzustellen, dass KI verantwortungsbewusst und effektiv ins Bildungssystem integriert wird. Basierend auf dieser Grundlage gibt das Sandbox-Team die folgenden Empfehlungen, um die Zukunft von KI in der Bildung gemeinsam zu gestalten:

Einheitliche Strategie für Rechtssicherheit

Die rechtlichen Rahmenbedingungen variieren derzeit von Kanton zu Kanton. Eine einheitliche, landesweite Strategie und Regelung würde zur Rechtssicherheit und Konsistenz im Umgang mit KI-Anwendungen beitragen. Dies würde eine klare und verständliche Grundlage für die Integration und Nutzung von KI-Technologien in Schulen schaffen und somit den Einsatz dieser Technologien in der gesamten Schweiz erleichtern.

Kantonale oder regionale Anlaufstellen für KI-Anbieter

Es wäre zielführend, kantonale oder regionale Anlaufstellen zu schaffen, bei denen KI-Anbieter ihre Produkte auf Datenschutzkonformität überprüfen lassen können. Dies würde Wiederholungen und Doppelspurigkeiten vermeiden, indem es einzelnen Schulen erspart würde, parallel mit verschiedenen Anbietern die gleichen Fragen zu klären. Des Weiteren können solche Anlaufstellen wichtige Schnittstellen zwischen Theorie und Praxis sein, um aktuell bestehende Diskrepanzen zu überwinden.

Verfolgung eigener Zwecke bei der KI-Produkt-Entwicklung

Es besteht eine erhebliche Unsicherheit bezüglich der Weiterverwendung von Daten und urheberrechtlich geschützten Werken für die Entwicklung von KI-Lösungen. Daher ist ein intensiverer politischer und gesellschaftlicher Diskurs erforderlich, um zu klären, inwiefern es Herstellern ermöglicht werden sollte, Personendaten und geschützte Werke für innovative Entwicklungen im Bildungsbereich, für eigene Zwecke und für kommerzielle Aktivitäten zu nutzen. Hierbei sollte insbesondere die Balance zwischen Innovationsförderung und Schutz von persönlichen und geistigen Eigentumsrechten beachtet werden.

Diese Empfehlungen sollen zur Entwicklung einer umfassenden und zukunftsfähigen Strategie für den Einsatz von KI im Bildungsbereich in der Schweiz beitragen. Sie bilden die Grundlage für einen breiten und tiefgreifenden Dialog zwischen allen Beteiligten, um das Thema KI im Bildungsbereich harmonisiert und konstruktiv angehen zu können.

Beteiligte Personen und Organisationen

Experteninterviews und inhaltliche Zusammenarbeit

René Moser, Volksschulamt Kanton Zürich
Nelly Buchser, Educa
Karen Grossmann, Educa
Manuel Brogli, Kellerhals Carrard
Verena Rohrer, Swiss EdTech Collider
Carmen Sieber, Swiss EdTech Collider
Moria Zürrer, Schulleiterin & Präsidentin Schule Medien Informatik Zürich

Autorin und Autor

Dr. iur. Stephanie Volz,
Rechtsexpertin Innovation-Sandbox für KI, Geschäftsführerin ITSL Universität Zürich

Raphael von Thiessen,
Leiter Innovation-Sandbox für KI, Standortförderung Kanton Zürich

Fallbeispiele aus der Innovation-Sandbox für Künstliche Intelligenz (KI)

Als Fallbeispiel innerhalb der Innovation-Sandbox für KI diente das Unternehmen Herby Vision AG. Die Organisation hat im Frühling 2022 einen Projektvorschlag in die Sandbox eingereicht. Herby bietet automatisierte Korrekturen von Primarschulaufgaben an, indem handgeschriebene Lernhinhalte durch KI-basierte Bilderkennung überprüft werden. Dank dem Testbed-Programm des Swiss Edtech Colliders konnte Herby sein Angebot an verschiedenen Schulen testen. Die Inhalte des vorliegenden Leitfadens wurden zwischen Juli 2022 und September 2023 basierend auf der konkreten Anwendung erarbeitet.

Impressum

Herausgeber
Standortförderung AWA, Kanton Zürich
Verein Metropolitanraum Zürich
Innovation Zurich

Projektkonzeption und -koordination
Raphael von Thiessen
Standortförderung Kanton Zürich
8090 Zürich
raphael.vonthiessen@vd.zh.ch

Konzeption in Zusammenarbeit mit:
Stephanie Volz
Isabell Metzler
Patrick Arnecke

Autorin und Autor
Dr. iur. Stephanie Volz
Raphael von Thiessen

Gestaltung
Sibylle Brodbeck, sibyllebrodbeck.ch

Publikation
Dieser Report erscheint ausschliesslich digital und in den Sprachen Deutsch und Englisch

Projekt-Steering
- Standortförderung im Amt für Wirtschaft und Arbeit, Kanton Zürich
- Statistisches Amt, Kanton Zürich
- Digitale Verwaltung und E-Government, Staatskanzlei Kanton Zürich
- Amt für Wirtschaft, Kanton Schwyz
- Metropolitanraum Zürich
- ETH AI Center
- UZH Center for Information Technology, Society, and Law (ITSL)
- swissICT
- ZHAW entrepreneurship