Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Leitlinien «Künstliche Intelligenz» für den Bund

Orientierungsrahmen für den Umgang mit künstlicher Intelligenz in der Bundesverwaltung

1 Kontext und Grundlagen

Auf der Grundlage des Berichts «Herausforderungen der künstlichen Intelligenz» vom 13. Dezember 2019[1] hat der Bundesrat das WBF beauftragt, in Zusammenarbeit mit dem UVEK und der Interdepartementalen Arbeitsgruppe künstliche Intelligenz **strategische Leitlinien für den Umgang mit den Herausforderungen der Künstlichen Intelligenz (KI) auf Ebene des Bundes** auszuarbeiten.

KI ist als **Grundlagentechnologie** ein wesentlicher Bestandteil der Digitalisierung von Staat, Wirtschaft und Gesellschaft. Der Bundesrat misst der künstlichen Intelligenz für die digitale Transformation eine grosse Bedeutung zu. Sie weist ein erhebliches **Innovations- und Wachstumspotenzial** auf. Entsprechend sind gute Rahmenbedingungen für deren Anwendung entscheidend. KI führt aber auch zu **spezifischen Herausforderungen**. Dazu gehören u.a. das Risiko von datenbasierter Diskriminierung bei KI-Entscheidungen sowie die Nachvollziehbarkeit von Ergebnissen. Auch muss der Schutz der Privatsphäre bei KI gewährleistet werden.

KI ist ein wichtiges Instrument für die Realisierung der Ziele des Bundesrates für die digitale Transformation und den Aufbau der digitalen Infrastrukturen in der Bundesverwaltung.[2] Die vorliegenden Leitlinien dienen als **allgemeiner Orientierungsrahmen** für den Umgang mit KI in der Bundesverwaltung und sollen eine **kohärente Politik gewährleisten**. Sie sollen der Bundesverwaltung sowie den Trägern von Verwaltungsaufgaben des Bundes eine Orientierung spezifisch in folgenden Kontexten geben:

- bei der Erarbeitung sektoraler KI-Strategien mit dem Ziel, Kohärenz in der KI-relevanten Politik des Bundes zu erreichen;
- bei der Einführung oder Anpassung von spezifischen Regulierungen in allen sektoralen Anwendungsbereichen, die von KI betroffen sind;
- bei der Entwicklung und beim Einsatz von KI-Systemen in Arbeitsbereichen des Bundes;
- bei der Mitgestaltung des internationalen Regelwerks zu KI.

Die Strategie «Digitale Schweiz» vom September 2020 gibt als **Dachstrategie** die Leitlinien für das staatliche Handeln im Bereich Digitalisierung vor. Sie will den Strukturwandel durch die digitale Transformation erleichtern, Chancen aktiv nutzen und den Risiken adäquat begegnen und wird entsprechend regelmässig aktualisiert. Die Grundsätze der Strategie gelten auch als Referenzrahmen für den Umgang mit KI. Ein weiteres Grundlagendokument für die Leitlinien KI ist die Strategie Digitalaussenpolitik 2021-2024 vom November 2020. Sie definiert die konzeptionellen Grundlagen für die Mitgestaltung der *internationalen* Gouvernanz im Bereich der Digitalisierung.

Das vorliegende Dokument definiert in Kapitel 2 **sieben grundlegende Leitlinien** für den Umgang mit KI. Kapitel 3 legt dar, wie die weitere Entwicklung der KI zu verfolgen ist.

Den Bereichen Bildung, Wissenschaft und Innovation kommt eine grosse Bedeutung zu, im Hinblick auf die Kompetenzen zur Nutzbarmachung des Innovations- und Wachstumspotenzials von KI sowie zur Bewältigung der ökologischen und gesellschaftlichen Herausforderungen. Für diese Politikbereiche sind daher spezifische Leitlinien in Anhang 1 dargestellt. Zudem ist im Kontext der gesellschaftlichen Herausforderungen zu beachten, dass die bestehende

[1] Bericht der interdepartementalen Arbeitsgruppe künstliche Intelligenz an den Bundesrat (2019): «Herausforderungen der künstlichen Intelligenz».

[2] Bundesrat (2019): «Zielbild für die digitale Transformation in der Bundesverwaltung und den Aufbau der digitalen Infrastrukturen».

Rechtsordnung vollumfänglich auch für die Anwendung von KI Geltung hat (Erläuterungen in Anhang 2).

2 Leitlinien für den Umgang mit KI

Die Grundlage für den Umgang mit KI ist die für die Schweiz geltende nationale und internationale Rechtsordnung, insbesondere die Bundesverfassung der Schweizerischen Eidgenossenschaft (BV, SR 101) und die Normen der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK). Darüber hinaus sind im Umgang mit KI folgende Leitlinien zu beachten, die je nach Anwendungskontext unterschiedlich stark zum Tragen kommen:[3]

Leitlinie 1: Den Menschen in den Mittelpunkt stellen

Bei der Entwicklung und beim Einsatz von KI sollen die **Würde und das Wohl des einzelnen Menschen sowie das Gemeinwohl** an vorderster Stelle stehen. Die Selbstbestimmung soll gewahrt werden: Die Menschen sollen in der Lage sein, sich in eigenverantwortlicher und autonomer Weise im politischen und gesellschaftlichen Leben einzubringen. Der Einsatz von KI soll dabei helfen, die Lebensqualität der Menschen zu steigern und unsere Gesellschaft aus sozialer, politischer, wirtschaftlicher und umweltpolitischer Perspektive nachhaltig weiter zu entwickeln. Hierbei soll durch den Einsatz von KI die Chancengleichheit der Menschen unterstützt und deren Zugang zu Bildung, Gütern, Dienstleistungen und Technologie gefördert und erleichtert werden.

Besondere Bedeutung kommt beim Einsatz von KI dem Schutz der **Grundrechte** zu. In die Gestaltung und Anwendung von KI müssen auch grundrechtliche und ethische Überlegungen einfliessen («ethics by design»). KI-Anwendungen, bei denen eine Tangierung der Grundrechte wahrscheinlich ist, sollen durch eine Folgenabschätzung, eine fortlaufende Beobachtung und angemessene Schutzmassnahmen und Kontrollen ergänzt werden, insbesondere bei selbstlernenden Systemen.[4]

So müssen Personen, Gruppen und Geschlechter vor **Diskriminierung** und Stigmatisierung geschützt werden. Dazu müssen angemessene technische und organisatorische Schutzmassnahmen und Kontrollen vorgesehen, ausgewogene und qualitativ hochwertige Daten verwendet oder entsprechende flankierende Schutzmassnahmen getroffen werden.

KI-Technologien, welche durch den Bund genutzt werden, müssen so konzipiert werden, dass die **Privatsphäre** standardmässig geschützt wird und die **Datenschutzbestimmungen** stets einhalten werden (vgl. auch Anhang 2).

Leitlinie 2: Rahmenbedingungen für Entwicklung und Anwendung von KI

Der Bund muss weiterhin bestmögliche Rahmenbedingungen gewährleisten, sodass die Chancen der KI genutzt werden können. Die Schweiz soll sich zu einem führenden, innovativen Standort für Forschung, Entwicklung, Anwendung und Unternehmen im Bereich KI weiterentwickeln. KI soll dazu beitragen, im Sinne der nachhaltigen Entwicklung eine hohe Lebensqua-

[3] Die Leitlinien lehnen sich an die Arbeiten der OECD, des Europarats und der EU an, siehe:
- «OECD-Grundsätze für KI», Mai 2019 (LINK)
- «Empfehlung des Ministerkomitees des Europarats zu den menschenrechtlichen Auswirkungen von algorithmischen Systemen», April 2020 (LINK)
- «On Artificial Intelligence – A European approach to excellence and trust», Februar 2020 (LINK),
- «Ethik-Leitlinien für eine vertrauenswürdigende KI» der Unabhängigen und hochrangigen Expertengruppe für KI, eingesetzt von der Europäischen Kommission, Juni 2018 (LINK).

[4] Für die Folgenabschätzung könnte man sich an bestehenden Instrumenten wie der Regulierungsfolgenabschätzung (RFA) (LINK), der Gleichstellungsfolgenabschätzung {LINK} und der im neuen Datenschutzgesetz (DSG) vorgesehenen Datenschutz-Folgenabschätzung orientieren.

lität sicherzustellen, wobei die Agenda 2030 den allgemeinen Orientierungsrahmen darstellt. Um alle diese verschiedenen Ziele erreichen zu können, ist ein ausbalancierter Regulierungsansatz erforderlich.

Die Fortsetzung einer **technologieneutralen Regulierung** durch den Bund, welche Spielräume für Innovation zulässt, aber auch eine demokratisch legitimierte und verantwortungsvolle Anwendung neuer Technologien sicherstellt, hohe Rechtssicherheit und die gute Reputation der Schweiz als Forschungs- und Innovationsstandort sind Erfolgsfaktoren für die Positionierung der Schweiz im Bereich der KI. Diese bewährten Rahmenbedingungen sorgen dafür, dass die Schweiz auch bei dieser Grundlagentechnologie die Chancen ergreifen und ihre gute Ausgangslage für die erfolgreiche Anwendung der Technologien nutzen kann.

Auch bei KI soll die Entscheidung über die **Wahl spezifischer Technologien** den Akteuren in Wirtschaft und Wissenschaft überlassen werden. Aufgabe der Politik ist es, für die Akteure die erforderlichen Freiräume zu schaffen, aber auch den erforderlichen Rahmen und die notwendigen Grenzen zu setzen.

Bildung, Forschung und Innovation sind eine zentrale Grundlage der hohen Wettbewerbsfähigkeit der Schweiz. Die Kompetenzen in diesen Bereichen sind im Hinblick auf die Nutzung des Anwendungs- und Innovationspotenzials von KI zu stärken. Forschung und Innovation soll möglichst hindernisfrei möglich sein und Grundlagen schaffen für eine verantwortungsvolle Entwicklung von KI.[5] Innovationen sind im Rahmen der etablierten Organe der Innovationsförderung und unter Verwendung des bewährten Prinzips des „bottom-up“ zu unterstützen.

Die Potenziale für **wirtschaftliches Wachstum, Wohlstand, Sicherheit und Beschäftigung** sowie für die **Reduzierung des ökologischen Fussabdrucks und des Energieverbrauchs**, die durch KI möglich werden, sollen optimal genutzt werden können. Die Wirtschaft soll ausreichend Raum für Effizienzgewinne und zur Entfaltung neuer Geschäftsmodelle haben und die Rahmenbedingungen für digitale Lösungen sind so auszugestalten, dass Innovationen nicht behindert werden und diese zu einer Stärkung der Wertschöpfung und zu einer nachhaltigen Entwicklung beitragen.

Leitlinie 3: Transparenz, Nachvollziehbarkeit und Erklärbarkeit

Transparenz, Nachvollziehbarkeit und Erklärbarkeit sind Grundvoraussetzungen für vertrauenswürdige KI. Eine auf KI gestützte Entscheidungsfindung sowie die Interaktion mit KI-Systemen sollen als solche klar erkennbar sein. Um die Einhaltung anderer Prinzipien sowie fundamentaler Grund- und Menschenrechte garantieren zu können, soll die Funktionsweise von KI sowie deren Zweck in verantwortungsvoller und rechtskonformer Weise offengelegt werden. Zusätzlich sollen die Datensätze, welche zum Training oder Entwicklung von KI verwendet werden, im Rahmen der gesetzlichen Verpflichtungen offengelegt werden, um eine Kontrolle zu ermöglichen. Auf KI gestützte Entscheidungsprozesse sollten so gestaltet sein, dass sie für direkt und indirekt betroffene Personen nachvollziehbar sind und die Wirkungsweise für Fachleute überprüfbar sind. Dies gilt insbesondere für Prozesse, die zu ethisch bedenklichen KI-Entscheidungen führen können. Dabei ist zu berücksichtigen, dass bei einigen KI-Methoden die Nachvollziehbarkeit eine grundsätzliche Herausforderung darstellt.

Die **Datenpolitik** muss eine Balance zwischen dem Schutz der Persönlichkeit und der Nutzung von Daten gewährleisten. Sie soll darauf hinwirken, dass Daten, welche für Anwendungen im Bereich KI genutzt werden, eine ausreichende Qualität und Dokumentation haben. Darunter fällt eine zweckgebundene Erhebung und Verwendung von Daten («fit for purpose») nach ethi-

[5] Die spezifischen Leitlinien für die Politikbereiche Bildung und Wissenschaft dienen als Basis, um die Kompetenzen in diesen Bereichen im Hinblick auf die gesellschaftliche Verantwortung zu schärfen. Diese sind in Anhang 1 dargestellt.

schen Standards sowie insbesondere auch die Sicherung der Interoperabilität der Datensysteme. Das Datenschutzgesetz sieht darüber hinaus eine Transparenzpflicht im Zusammenhang mit automatisierten Entscheidungen vor (vgl. Anhang 2 II).

Leitlinie 4: Verantwortlichkeit

Um im Falle eines Schadens, eines Unfalls oder einer Gesetzeswidrigkeit die Verantwortlichkeiten klären und feststellen zu können, muss beim Einsatz von KI **die Haftung klar definiert sein**. Die Verantwortlichkeit darf nicht an Maschinen delegiert werden können.

Leitlinie 5: Sicherheit

KI-Systeme müssen **sicher, robust und resilient** konzipiert sein, um sich positiv auf die Menschen und die Umwelt auszuwirken und nicht anfällig für Missbrauch oder Fehlanwendungen zu sein. Zur Vermeidung von schwerwiegenden Fehlentscheidungen müssen geeignete Massnahmen existieren. Wo immer sinnvoll, soll auf dezentral vernetzte KI-Systeme abgestützt werden. Durch angemessenes Verfolgen und Beurteilen der Auswirkungen des Einsatzes von KI sollen die Risiken für den einzelnen Menschen, die Gesellschaft, die Wirtschaft und die Umwelt frühzeitig identifiziert und ausgeschlossen oder minimiert werden.[6]

Leitlinie 6: Aktive Mitgestaltung der Gouvernanz von KI

Für die Schweiz als hochentwickeltes und hochvernetztes Land ist es zentral, die **globale Gouvernanz von KI aktiv mitzugestalten**. Sie soll sich daher in den relevanten internationalen Organisationen und Prozessen, wie UNO, OECD, ITU, UNESCO, Europarat und Partnership for Peace (PfP), weiterhin engagieren, insbesondere bei der Erarbeitung von globalen Standards und Normen zum Umgang mit KI. Gleichzeitig muss sie auch die Entwicklungen innerhalb der EU und der NATO mitverfolgen. Die Schweiz soll sich dabei gemäss ihren Interessen und ihren Werten einbringen. Sie soll sich insbesondere dafür einsetzen, dass bei der Entwicklung und beim Einsatz von KI auch auf internationaler Ebene bestehende Verpflichtungen und Standards – namentlich in den Bereichen Menschenrechte und verantwortungsvolle Unternehmensführung[7] – respektiert werden.

Leitlinie 7: Einbezug aller relevanten nationalen und internationalen Akteure

Die Schweiz soll sich dafür einsetzen, dass in den Debatten um die Gouvernanz von KI **alle relevanten Anspruchsgruppen** – nebst den Staaten auch die Privatwirtschaft, die Zivilgesellschaft und die technischen und wissenschaftlichen Expertinnen und Experten – aus aller Welt (auch aus Entwicklungsländern) in **die politischen Entscheidungsprozesse einbezogen** und bei deren Umsetzung wirksam in die Pflicht genommen werden können. Im Einklang mit ihren aussenpolitischen Prioritäten fördert die Schweiz dabei insbesondere auch die Vernetzung und die sektorübergreifende Zusammenarbeit der Akteure zu KI, mit dem Ziel, Genf als Zentrum für digitale Gouvernanz von KI zu stärken.

---

[6] Insbesondere bei Risiko- und Verwundbarkeitsanalysen sollen die Massnahmen der nationalen Strategien zum Schutz kritischer Infrastrukturen (SKI) (LINK) sowie zum Schutz der Schweiz vor Cyber-Risiken (NCS) (LINK) zur Anwendung kommen.

[7] Die wichtigsten internationalen Standards zur verantwortungsvollen Unternehmensführung sind die UN-Leitprinzipien für Wirtschaft und Menschenrechte, die OECD-Leitsätze für multinationale Unternehmen und die Dreigliedrige Grundsatzerklärung der IAO über multinationale Unternehmen und Sozialpolitik.

3 Verfolgen der weiteren Entwicklung von KI

Angesichts der hohen technologischen Dynamik soll die weitere Entwicklung von KI aufmerksam und kontinuierlich verfolgt und wo nötig intensiviert werden.[8] Dies hat im Rahmen der Sektoralpolitik in Zuständigkeit der jeweiligen Ämter zu geschehen. Zur Gewährleistung der Kohärenz sind die vorliegenden Leitlinien zu berücksichtigen. Wichtig ist ausserdem der **Dialog und der Informations- und Wissensaustausch** zwischen allen Anspruchsgruppen über die sektorspezifischen Herausforderungen und die eingeleiteten Massnahmen mit Bezug zu KI.

In Anbetracht der globalen Dimension von KI wird der Dialog sowohl auf nationaler, als auch auf internationaler Ebene geführt. Insbesondere stellen internationale Foren, in denen auch die Schweiz vertreten ist, einen wichtigen Rahmen dar, um grundlegende Fragen rund um die weitere Entwicklung und den Einsatz von KI zu formen und zu begleiten und ein angemessenes Monitoring sicherzustellen.

Die **Aktualität und Anwendbarkeit der vorliegenden Leitlinien muss gewährleistet bleiben.** Eine regelmässige Beurteilung in Bezug auf ihre Anwendung und allfällige Anpassungen sind mit der Strategie «Digitale Schweiz» und der Strategie Digitalaussenpolitik 2021-2024 abzustimmen.

[8] Der Bericht «Herausforderungen der künstlichen Intelligenz» vom Dezember 2019 hat im Detail aufgezeigt, in welchen Politikfeldern die verschiedenen Bundesstellen dies bereits tun und welchen spezifischen Herausforderungen und Sachfragen sie sich bereits annehmen.

Anhang 1: Spezifische Leitlinien im Politikbereich Bildung, Forschung und Innovation

Zu den wesentlichen Rahmenbedingungen für eine erfolgreiche Nutzung von KI zählen die Kompetenzen in **Bildung, Wissenschaft und Innovation**.

KI bringt enorme Chancen zur Verbesserung von **Lehr- und Lernprozessen** mit sich. Gleichzeitig hat KI Folgen für die Kompetenzen, die die Bürgerinnen und Bürger besitzen müssen, um in einer digitalisierten Gesellschaft leben und arbeiten zu können. Das Bildungssystem muss den angemessenen Erwerb von Grundkompetenzen für alle sowie den Erwerb spezifischer Kompetenzen zur Produktion von KI-Systemen sicherstellen und folglich auch zur Ausbildung von KI-Spezialistinnen und -Spezialisten beitragen.

Damit sich die Anwendung von KI bestmöglich zum Wohle der Gesellschaft im Sinne einer nachhaltigen Entwicklung entfaltet, kommt der **Wissenschaft** eine zentrale Rolle zu. Diese liefert einerseits die **Grundlagen für die Weiterentwicklung von KI-Technologien**, um die ein intensiver globaler Wettbewerb besteht. Sie erforscht andererseits KI-Anwendungen, welche ermöglichen, dass KI einen entscheidenden Beitrag zur Bewältigung der grossen gesellschaftlichen Herausforderungen leisten kann. Gleichzeitig sollen auf Basis neuer wissenschaftlicher Erkenntnisse allfällige Risiken und Probleme, die mit KI einhergehen, verhindert oder gemindert werden.

Damit die Chancen der KI bestmöglich genutzt werden und sich die Schweiz als ein führender Standort für Forschung, Entwicklung und Anwendung von KI etablieren kann, müssen die **Kompetenzen in Bildung, Forschung und Innovation mit den Entwicklungen Schritt halten und gestärkt werden**. Dabei sind die Grundsätze der Technologie- und Innovationspolitik des Bundes zu beachten, welche sich bislang auch im Kontext der dynamischen technologischen Entwicklung von KI bewährt haben:

- **Grundsätzlich technologieneutraler Ansatz**

  Der Bund gibt nicht vor, welche Technologien in Bildung, Wissenschaft und Wirtschaft angewendet werden sollen und verzichtet weitgehend auf eine Förderung spezifischer Technologien. Die Politik soll für optimale, innovationsfreundliche Rahmenbedingungen sorgen, welche die Entfaltung neuer Technologien ermöglichen. Eine solche Offenheit des Staates gegenüber neuen Technologien erlaubt das optimale Ausschöpfen des Potenzials von neuen Ideen und Innovationen. Um Transparenz, Nachvollziehbarkeit und Erklärbarkeit zu unterstützen, soll beim Einsatz von KI – soweit möglich – offenen Systemen der Vorzug gegeben werden; dies gilt insbesondere für die Anwendung in Bildung und Wissenschaft.

- **Bottom-Up Ansatz**

  Die Entscheidung über die Wahl spezifischer Technologien bleibt den individuellen Akteuren in Bildung, Wissenschaft und Wirtschaft überlassen. Aufgabe der Politik ist es, für die Akteure die erforderlichen Freiräume und Voraussetzungen zu schaffen. Ein hoher Grad an Autonomie der Akteure und der Wettbewerb zwischen ihnen sorgen dafür, dass die Verantwortung durch die Akteure wahrgenommen werden kann.

Damit Wissenschaft und Bildung den grösstmöglichen Beitrag zum gesellschaftlichen Wohlergehen beisteuern können, sollen bei der Erforschung der Anwendung von KI auch die **gesellschaftlichen und ökologischen Auswirkungen** in ihrer ganzen Breite berücksichtigt werden. Dabei stehen u.a. die folgenden Dimensionen im Mittelpunkt:

- **Grundlagen der künstlichen Intelligenz**

  Wesentliche Elemente der KI aus methodischer Sicht sind offen. Sie werden die Tragweite und die Einsatzmöglichkeiten dieser Technologien quantitativ und qualitativ

grundlegend verändern. Es ist daher essenziell, neben Anwendungen von KI auch die methodischen Grundlagen zu erweitern.

- **Ethische, rechtliche und gesellschaftliche Normen und Werte**

  Die Wissenschaft soll dazu beitragen, dass bei der Forschung zu KI die gesellschaftlichen und ökologischen Auswirkungen berücksichtigt werden und dass KI-Systeme entworfen und angewendet werden, welche die rechtlichen Normen sowie ethische und gesellschaftliche Ansprüche und Werte berücksichtigen.

- **Zusammenarbeit von Mensch und KI**

  Die Wissenschaft und die Bildung sollen das Verständnis für eine KI verbessern, welche ein erfolgreiches Zusammenarbeiten mit Menschen ermöglicht und so deren Tätigkeiten und Kompetenzen ergänzen und verbessern.

- **Akzeptanz von KI**

  Die Wissenschaft soll durch aktiven Dialog mit der Gesellschaft und einer Stärkung der Kompetenzen (insbes. auch im Bereich der Data Literacy) das Verständnis für KI, sowie für die mit der Anwendung von KI einhergehenden Chancen und Risiken fördern.

Die in diesem Kontext bestehenden Herausforderungen von KI sind durch Wissenschaft und Bildungsinstitutionen in ihrem Zuständigkeitsbereich anzugehen. Insbesondere sind Leitlinien für die eigene Anwendung von KI im Wissenschafts- und Bildungsbereich, die Investitionen in die Forschung und die Forschungsprioritäten bei Bedarf von den zuständigen Gremien und Hochschulen selbst zu etablieren.

Anhang 2: Anwendbarkeit der geltenden Rechtsordnung

I. Generell geltende Normen

KI entwickelt sich in einer bereits bestehenden Rechtsordnung, die auch für sie gilt. Diese Rechtsordnung besteht aus internationalen und nationalen Normen. In diesem Anhang werden einige wichtige Regelwerke vorgestellt, deren technologieneutrale Bestimmungen auch für KI zur Anwendung kommen. Ein Teil ist spezifisch dem neuen Datenschutzgesetz gewidmet, das besondere Massnahmen für KI vorsieht. Die folgende Liste ist nicht abschliessend.

- **Grundrechte und Menschenrechte:**

  Die Grundrechte müssen in der gesamten Rechtsordnung eingehalten werden. Sie sind in den Artikeln 7 ff. der Bundesverfassung aufgeführt (BV, SR 101). Das Völkerrecht wie etwa die Europäische Menschenrechtskonvention (EMRK; SR 0.101) und der Internationale Pakt über bürgerliche und politische Rechte (SR 0.103.2) sehen analoge Garantien vor. Die Grundrechte müssen in der ganzen Rechtsordnung zur Geltung kommen (Art. 35 BV). Ausserdem muss jegliche Einschränkung der Grundrechte den Voraussetzungen von Artikel 36 BV entsprechen. Die Einhaltung der Prinzipien des humanitären Völkerrechts ist jederzeit zu gewährleisten. So ist bei der Entwicklung neuer Waffen die Konformität mit dem humanitären Völkerrecht sicherzustellen.

- **Schutz des geistigen Eigentums:**

  Der Bereich des geistigen Eigentums ist ebenfalls wichtig für KI, insbesondere bei der Bearbeitung oder Nutzung von Daten, die durch das Urheberrecht geschützt sind. Hier gilt es, das Bundesgesetz über die Erfindungspatente (Patentgesetz, PatG; SR 232.14), das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG; SR 231.1) und die verschiedenen rechtlichen Bestimmungen zum Geschäftsgeheimnis zu berücksichtigen.

- **Zivil- und strafrechtliche Verantwortung:**

  Da Roboter keine Rechtspersönlichkeit haben, haftet eine natürliche oder juristische Person für durch KI entstandene Schäden, wenn die Haftungsvoraussetzungen erfüllt sind. So können etwa Verkehrsunfälle oder medizinische Fehler Haftungsfälle darstellen, die auf den Einsatz einer KI-basierten Software zurückzuführen sind. Diesbezüglich gelten unter anderem das Obligationenrecht (OR; SR 220), das Schweizerische Strafgesetzbuch (StGB; SR 311.0) oder das Bundesgesetz über die Produktehaftpflicht (Produktehaftpflichtgesetz, PrHG; SR 221.112.944).

- **Diskriminierungsverbot:**

  Die Bestimmungen zum Diskriminierungsverbot und zur Förderung der Gleichstellung gelten selbstverständlich auch für den Bereich der KI. Insbesondere Artikel 8 Absatz 2 und 3 der BV, das Bundesgesetz über die Gleichstellung von Frau und Mann (Gleichstellungsgesetz, GIG; SR 151.1), das Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (Behindertengleichstellungsgesetz, BehiG; SR 151.3), Artikel 28 ff. des Schweizerischen Zivilgesetzbuchs (ZGB; SR 210) über den Schutz der Persönlichkeit, der Internationale Pakt über wirtschaftliche, soziale und kulturelle Rechte (SR 0.103.1), das internationale Übereinkommen zur Beseitigung jeder Form von Rassendiskriminierung (SR 0.104) sowie das Übereinkommen über die Rechte von Menschen mit Behinderungen (SR 0.109) können im KI-Bereich zur Anwendung kommen.

- **Produktesicherheit:**

  Das Bundesgesetz über die Produktesicherheit (PrSG; SR 930.11) regelt die Gewährleistung der Produktesicherheit und das gewerbliche oder berufliche Inverkehrbringen von Produkten. Durch das PrSG werden die Sicherheit und die Gesundheit der Verwenderinnen und Verwender sowie Dritter geschützt, nicht aber die Privatsphäre. Für vernetztes Spielzeug kommt in erster Linie die Verordnung des EDI über die Sicherheit von Spielzeug (VSS; SR 817.023.11) zum Tragen. Die VSS enthält nur Anforderungen hinsichtlich des Gesundheitsschutzes der Konsumentinnen und Konsumenten. Die Risiken im Zusammenhang mit der digitalen Vernetzung eines Spielzeugs sind in der Verordnung nicht abgedeckt. Für Risiken betreffend den Datenschutz oder die Privatsphäre bei Spielzeugen kommt das Bundesgesetz über den Datenschutz zur Anwendung.

II. Neues Datenschutzgesetz

Die Datenschutzgesetzgebung und vor allem die Revision des Datenschutzgesetzes (DSG; SR 235.1) spielen eine zentrale Rolle im KI-Bereich. Das revidierte DSG, das in der Herbstsession 2020 angenommen wurde, sieht verschiedene Massnahmen vor, die sich spezifisch auf KI auswirken könnten:

- **Der Begriff «Profiling»:**

  Das neue Gesetz definiert Profiling als «jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen» (Art. 5 Bst. f nDSG). Ein Profiling zieht bestimmte Konsequenzen nach sich (insbesondere die Notwendigkeit einer formellen gesetzlichen Grundlage, siehe Art. 34 Abs. 2 Bst. b des neuen DSG). Das Parlament hat in Art. 5 Bst. g ausserdem neu eine Legaldefinition für das « Profiling mit hohem Risiko » eingeführt. Dieser Begriff ist aber vor allem für den privatrechtlichen Bereich von Bedeutung. Die Anforderungen des neuen DSG an die gesetzlichen Grundlagen für das Profiling durch Bundesorgane sind im Vergleich zum Entwurf des Bundesrates unverändert geblieben.

- **Biometrische und genetische Daten:**

  Genetische Daten sowie biometrische Daten, die eine natürliche Person eindeutig identifizieren, gehören inzwischen zum Katalog der besonders schützenswerten Daten. Das hat Konsequenzen für KI-Anwendungen, die Technologien wie die Gesichtserkennung einsetzen. Auch für die Bearbeitung besonders schützenswerter Daten gelten bestimmte Voraussetzungen (insbesondere die Notwendigkeit einer formellen gesetzlichen Grundlage, vgl. Art. 34 Abs. 2 Bst. a des neuen DSG).

- **Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen («privacy by design / privacy by default»):**

  Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, und dies ab der Planung (Art. 7 des neuen DSG).

- **Pflicht zur Durchführung einer Folgenabschätzung:**

  Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte

mit sich bringen kann. Ein hohes Risiko besteht insbesondere bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden (Art. 22 des neuen DSG).

- **Informationspflicht bei einer automatisierten Entscheidung (Art. 21 und 25 Abs. 2 Bst. f des neuen DSG):**

  Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt. Darüber hinaus hat die betroffene Person das Recht, ihren Standpunkt darzulegen und kann verlangen, dass die Entscheidung von einer natürlichen Person überprüft wird. Diese Massnahmen gelten nicht, wenn die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt oder wenn die Entscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird. Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen. Das Recht der betroffenen Person, ihren Standpunkt darzulegen und zu verlangen, dass eine Entscheidung von einer natürlichen Person überprüft wird, gilt nicht, wenn die Person gemäss Artikel 30 Absatz 2 des Bundesgesetzes über das Verwaltungsverfahren oder gemäss einem anderen Bundesgesetz vor der Entscheidung nicht angehört werden muss. Bei der Ausübung ihres Auskunftsrechts erhält die betroffene Person insbesondere die Informationen zum Vorliegen einer allfälligen automatisierten Entscheidung und zur Logik, auf die sich diese Entscheidung stützt.

- **Notwendigkeit einer formellen gesetzlichen Grundlage:**

  Bundesorgane dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 34 des neuen DSG). Eine Grundlage in einem Gesetz im formellen Sinn ist in den folgenden Fällen erforderlich:

  - Es handelt sich um die Bearbeitung von besonders schützenswerten Personendaten;
  - Es handelt sich um ein Profiling;
  - Der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung können zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen. Der Einsatz von KI kann also auch dann eine formelle rechtliche Grundlage voraussetzen, wenn es nicht um die Bearbeitung besonders schützenswerter Daten oder um ein Profiling geht, sondern wenn die Art und Weise der Datenbearbeitung (z.B. automatisierte Entscheidung) zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen könnte.

  Artikel 34 Absatz 3 regelt die Ausnahmen.