# Potenzialanalyse zum Standardisierungsbedarf im Kontext von künstlichen Intelligenz (KI) in Verbindung mit eGovernment

| | |
|---|---|
| **Kategorie** | Potenzialanalyse |
| **Reifegrad** | offen |
| **Version** | 2.0 |
| **Status** | In Arbeit**;** Entwurf; **Vorschlag**; Genehmigt; Abgelöst; Aufgehoben, Sistiert |
| **Ausgabedatum** | 22.02.2022 (aktualisiert am 06.06.2022) |
| **Beilagen** | keine |
| **Sprachen** | Deutsch (Original) |
| **Autoren** | Robin Pekerman (eCH), Beiträge von Frauenhoferinstitut, BAKOM sowie Kompetenznetzwerk KI (CNAI) |
| **Herausgeber / Vertrieb** | Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich<br>T 044 388 74 64, F 044 388 71 80<br>www.ech.ch / info@ech.ch |

# Inhaltsverzeichnis



# Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

# 1 Management Summary

Künstliche Intelligenz (KI) wird als Schlüsseltechnologie des 21. Jahrhunderts betrachtet und wird in Zukunft das öffentliche Leben sehr stark prägen. Mit dieser Technologie werden neue Türen für die Wirtschaft und Gesellschaft geöffnet. Angesichts dieser Erkenntnisse hat der Bundesrat im Jahr 2018 das Thema «künstliche Intelligenz» als zentrales Thema der Strategie «Digitale Schweiz» definiert und eine interdepartementale Arbeitsgruppe gebildet, welche dann einen Bericht zum Thema «Herausforderungen der künstlichen Intelligenz» vorgelegt hat. Damit wurde die Bedeutung dieses Themenfelds auch im Bereich eGovernment aufgestuft.

Der Einsatz der künstlichen Intelligenz benötigt innovationsfreundliche Rahmenbedingungen. Diese Rahmenbedingungen müssen Standards und Normen enthalten, damit KI-Systeme für ihre Anspruchsgruppen verlässlich und sicher arbeiten. Daraus leitet sich auch der Bedarf einer Potenzialanalyse für Standards im Bereich «künstliche Intelligenz» ab, welcher für eCH künftig ein mögliches Themenfeld sein könnte. Mit der vorliegenden Potenzialanalyse hat eCH die Chancen von möglichen KI-Standards untersuchen lassen. Die Ergebnisse der analysierten Berichte und Beiträge zeigen, dass KI-Standards einerseits die Vertrauenswürdigkeit der KI-Anwendungen unterstützen und anderseits auch die Interoperabilität der KI-Systeme gewährleisten. Insbesondere im öffentlichen Bereich können KI-Standards wichtige Sicherheitsaspekte auch im Sinne der Rechtssicherheit abdecken sowie auch finanzielle Vorteile anbieten. Anhand dieser Potenzialanalyse stellt eCH ihren Gremien sowie auch weiteren Interessengruppen eine Entscheidungsgrundlage zur Verfügung, ob das Thema KI-Standards künftig bei eCH ein Bedarf hat. Die Potenzialanalyse enthält Beiträge vom Frauenhoferinstitut, Bundesamt für Kommunikation (BAKOM) und das Kompetenznetzwerk KI (CNAI) vom Bund.

Um die Chancen und Risiken der KI-Standards im Bereich eGovernment in der vorliegenden Analyse vollständig zu verstehen, müssen die Fragenstellungen, Antworten sowie die behandelten Themen in dieser Potenzialanalyse gesamtheitlich betrachtet werden. Da das Thema Standards und Normen im Bereich der künstlichen Intelligenz ein übergreifendes Thema ist, bilden deren Standardisierungsvorhaben, die ausserhalb des Bereichs eGovernment sind, auch wichtige Erkenntnisse für die vorliegende Analyse. Sollten KI-Standards künftig bei eCH kein Thema sein, so können die Anspruchsgruppen der eCH aufgrund dieser Analyse dennoch erfahren, wo KI-Standards geforscht und welche nationalen oder auch internationalen Organisationen die Einführung von KI-Standards beabsichtigen.

# 2 Auftrag/ Zielsetzung

Der Verein eCH entwickelt Standards im Bereich eGovernment, um eine effiziente Zusammenarbeit zwischen den Behörden, Unternehmen und Privat zu gewährleisten.

Mit der vorliegenden Analyse klärt der Verein eCH das Potenzial d.h. Chancen und Risiken der Standards im Bereich der künstlichen Intelligenz ab. Das Ziel der Potenzialanalyse ist in erster Linie die konzeptionelle Klärung, ob im Themenfeld «KI-Standards»

- ein Potenzial für die Einführung neuer Standards besteht.
- ein relevanter Nutzen mit der Einführung von neuen Standards zu erwarten ist.
- Stakeholder mit hohem Interesse an der Einführung von Standards identifizierbar sind.
- bereits (nationale und/oder internationale) Standards (oder de facto Standards) vorhanden sind (und genutzt werden).
- und welche Form von Standards zu welchen Themen dabei im Vordergrund steht (Datenaustausch-, Dokumenten-, Formate-, Methoden-, Architektur-Standards etc.)

Des Weiteren sollten folgende, weitere Fragen soweit wie möglich beantwortet werden:

- Welches die Organisationen oder Personen sein könnten, welche die Entwicklung entsprechender Standards vorantreiben könnten:
  - wie die Chancen für die erfolgreiche Erarbeitung von Standards eingeschätzt werden;
  - wie konkret weiter vorgegangen werden soll.
- Was sind die Chancen entsprechender Standards in der Schweiz? Inwieweit ist die Machbarkeit gewährleistet? (Möglich im internationalen Kontext? Möglich im Rahmen von spezifischen Phasen?)
- Sollten Standards in bestimmten Felder angestrebt werden? Welche Schlussfolgerungen ergeben sich für eCH?
- Ob die bereits vorhandenen Standards ausreichen oder ob Ergänzung bzw. die Einführung weiterer Standards grundsätzlich sinnvoll sind und einen massgeblichen Nutzen versprechen;

Die Beantwortung der oben genannten Fragestellung folgt einerseits aus den Studien und Berichten, die in den folgenden Kapiteln beschrieben werden und andererseits aus den Beiträgen den Projektteilnehmern, die ebenfalls in den folgenden Kapiteln zu finden sind.

# 3 Projektorganisation

Robin Pekerman ist Mitglied des Expertenausschusses eCH und Dozent für «künstliche Intelligenz». Im Auftrag von eCH hat er die vorliegende Potenzialanalyse zusammen mit den Experten aus dem In- und Ausland erarbeitet.

Das Projektteam setzte sich aus den folgenden Rollen und Aufgaben zusammen:

| **Rolle** | **Funktion** | **Name** |
|---|---|---|
| Projektleitung | Aufbau, Struktur, Recherche, Konsolidierung der Inhalte, Koordination der Projektteilnehmer, Studienanalyse<br>Kapitel 1, 2, 3, 4, 5, 7, 8 | Robin Pekerman, Mitglied des Expertenausschuss eCH, Dozent für künstliche Intelligenz sowie Mitglied der Arbeitsgruppe Normungsroadmap KI Deutschland |
| Projektmitarbeit:<br>Frauenhoferinstitut | Beitrag zum Thema KI-Standards:<br>Kapitel 6.1 | Maximilian Poretschkin, Teamleiter KI-Absicherung und –Zertifizierung von Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS |
| Projektmitarbeit:<br>Kompetenznetzwerk Bund | Beitrag zum Thema KI-Standards:<br>Kapitel 6.2 | Diego Kuonen, Leiter ad interim Geschäftsstelle Kompetenznetzwerk KI (CNAI) |
| Projektmitarbeit:<br>BAKOM | Beitrag zum Thema KI-Standards:<br>Kapitel 6.3 | BAKOM |

**Vorgehensbeschrieb**

Anhand eines Desk-Researchs wurden die Fragenstellungen, welche im Kapitel Auftrag beschrieben sind, soweit wie möglich beantwortet. Die Beantwortung der Fragestellung erfolgt einerseits aus der Analyse der Studien und Berichte und andererseits aus den Beiträgen der Experten im In- und Ausland.

# 4 Begriffsdefinitionen

In diesem Kapitel werden nicht alle Begriffsdefinition dieser Analyse beschrieben. Es werden lediglich Begriffsdefinitionen erläutert, die für die Analyse von Bedeutung sind.

## 4.1 Künstliche Intelligenz

Künstliche Intelligenz beschreibt die Fähigkeit einer Maschine, kognitive Aufgaben auszuführen, die wir mit dem menschlichen Verstand verknüpfen. Dazu zählen die Möglichkeiten zur Wahrnehmung sowie Fähigkeiten zur Argumentation, zum selbständigen Lernen und damit zum eigenständigen Finden von Problemlösungen (Kreutzer & Sirrenberg, 2019, S. 3).

## 4.2 Maschinelles Lernen

Der Begriff "Maschinelles Lernen" befasst sich mit Methoden, die anhand von Lernprozessen Zusammenhänge in bestehenden Datensätzen erkennen, um darauf aufbauend Vorhersagen abzuleiten (Murphy, 2012; zitiert nach Buxmann & Schmidt, 2019, S. 8).

## 4.3 Standards und Normen

Standards bzw. Standardisierung ist die Ausarbeitung von Spezifikationen durch eine temporär zusammengestellte Arbeitsgruppe. Im Vergleich zur Normung sind der Konsens aller Beteiligten, die Einbeziehung aller Anspruchsgruppen sowie eine Entwurfs-Veröffentlichung nicht zwingend notwendig ([VDE] Verband der Elektrotechnik Elektronik Informationstechnik e. V., 2020).

Laut Wikipedia (n.d) ist ein Standard eine vergleichsweise einheitliche oder vereinheitlichte, weithin anerkannte und meist angewandte (oder zumindest angestrebte) Art und Weise, etwas zu beschreiben, herzustellen oder durchzuführen, die sich gegenüber anderen Arten und Weisen etabliert bzw. erwiesen hat oder zumindest als Richtschnur existiert.

Normung ist die planmässige, durch die Anspruchsgruppen zusammen durchgeführte Vereinheitlichung materiellen und immateriellen Gegenständen zum Nutzen der Allgemeinheit. Die Normung besitzt dank ihrer bewährten Prozesse eine Legimitation und ist kartellrechtlich unbedenklich (VDE, 2020).

## 4.4 eGovernment

eGovernment beschreibt den Einsatz von digitalen Informations- und Kommunikationstechnologien, damit die Bevölkerung und Wirtschaft wichtige Geschäfte mit den Behörden digital ausführen können. eGovernment leistet einen wichtigen Beitrag auf dem Weg zur Modernisierung der Verwaltung (eGovernment Schweiz, n.d.).

# 5 Aktuelle Studien und Berichte

## 5.1 Entwurf Verordnung der EU-Kommission KI Regulierung

Die Europäische Kommission hat weltweit den ersten Vorschlag (Entwurf) für die Regulierung der künstlichen Intelligenz definiert. Dies hat die Kommission am 21.04.2021 der Öffentlichkeit mitgeteilt. Das Ziel der EU ist, ein Gesetz über die künstliche Intelligenz zu erlassen, das einen Rechtsrahmen zur künstlichen Intelligenz vorlegt. Damit will die EU eine führende Rolle im Bereich der KI-Regulierung übernehmen. Ähnlich wie bei der Datenschutz-Grundverordnung 2016/679, die für viele Unternehmen weltweit innerhalb eines kurzen Zeitraums zum Standard wurde, möchte die EU weitreichende Auswirkungen erzielen.

In erster Linie sollen folgende Ziele mit dem genannten Rechtsrahmen angestrebt werden:

- Es muss gewährleistet sein, dass die auf dem Unionsmarkt in Verkehr gebrachten und verwendeten KI-Systeme sicher sind und die bestehenden Grundrechte und die Werte der Union wahren.
- Zur Förderung von Investitionen in KI und innovativer KI muss Rechtssicherheit gewährleistet sein.
- Governance und die wirksame Durchsetzung des geltenden Rechts zur Wahrung der Grundrechte sowie die Sicherheitsanforderungen an KI-Systeme müssen gestärkt werden.
- Die Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen muss erleichtert werden und es gilt, eine Marktfragmentierung zu verhindern (Europäische Kommission, 2021, S. 3).

Folgend werden die zentralen Aspekte des Entwurfs aufgezeigt:

Gemäss Art. 3 Abs. Abs. 1 soll ein KI-System dann bereits vorliegen, wenn die Software mit einer der folgenden Konzepten und Techniken entwickelt wurde:

a) Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einem grossen Umfang von Methoden, inklusive des tiefen Lernens (Deep Learning)
b) Logik- und wissensgestützte Konzepte, inklusive Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, (symbolischer) Schlussfolgerungs- und Expertensysteme, Inferenz- und Deduktionsmaschinen;
c) Statistische Modelle, Bayessche Schätz-, Such- und Optimierungsmethoden (Europäische Kommission, 2021).

Laut Art. 5 soll der Einsatz von KI insbesondere in folgenden Bereichen verboten werden:

a) Der Einsatz, die Inbetriebnahme oder die Anwendung eines KI-Systems, das Techniken der unterschwelligen Beeinflussung ausserhalb des Bewusstseins einer Person einsetzt, um das Verhalten einer Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen physischen oder psychischen Schaden zufügt oder zufügen kann;
b) Der Einsatz, die Inbetriebnahme oder die Anwendung eines KI-Systems, das eine Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund ihres Alters oder

ihrer körperlichen oder geistigen Behinderung ausnutzt, um das Verhalten einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu beeinflussen, die dieser Person oder einer anderen Person einen physischen oder psychischen Schaden zufügt oder zufügen kann;

c) Der Einsatz, die Inbetriebnahme oder die Anwendung eines KI-Systems durch Behörden oder in deren Auftrag zur Bewertung oder Klassifizierung der Vertrauenswürdigkeit natürlicher Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale;

d) die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, ausser wenn und insoweit dies im Hinblick auf eines der Ziele wie Suche nach Opfern von Straftaten, Verfolgung eines Täters, Abwenden einer Gefahr wie Terroranschlag unbedingt erforderlich ist; (Europäische Kommission, 2021, S. 3)

Des Weiteren erwähnt der Verordnungsentwurf im Artikel 6 Klassifizierungsvorschriften für Hochrisiko-KI-Systeme. Demnach sind KI-Systeme, die in folgenden Bereichen eingesetzt werden, "Hochrisiko-KI-Systeme":

- Rechtspflege und demokratische Prozesse (zum Beispiel: Anwendung der Rechtsvorschriften auf konkrete Sachverhalte)
- Strafverfolgung, die in die Grundrechte der Menschen eingreifen könnte (zum Beispiel: Bewertung der Verlässlichkeit von Beweismitteln);
- kritische Infrastrukturen (zum Beispiel: Verkehr), in denen das Leben und die Gesundheit der Bürger gefährdet werden könnten;
- Schul- oder Berufsausbildung, wenn der Zugang einer Person zur Bildung und zum Berufsleben beeinträchtigt werden könnte (zum Beispiel: Bewertung von Prüfungen);
- Sicherheitskomponenten von Produkten (zum Beispiel: eine KI-Anwendung für die roboterassistierte Chirurgie);
- Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit (zum Beispiel: Software zur Auswertung von Lebensläufen für Einstellungsverfahren);
- wichtige private und öffentliche Dienstleistungen (zum Beispiel: Bewertung der Kreditwürdigkeit, wodurch Bürgern die Möglichkeit verwehrt wird, ein Darlehen zu erhalten);
- Migration, Asyl und Grenzkontrolle (zum Beispiel: Überprüfung der Echtheit von Reisedokumenten); (Europäische Kommission, 2021)

Gemäss Artikel 8 ff. sollen Hochrisiko-KI-Systeme bestimmte Anforderungen erfüllen, die im Verordnungsentwurf wie folgt definiert sind:

- Angemessene Risikomanagementsysteme, insbesondere Risikobewertungs- und Risikominderungssysteme, die im Artikel 9 erwähnt sind (Europäische Kommission, 2021, S. 54)
- Angemessene Datengovernance und Datenverwaltungsverfahren, vor allem hohe Qualität an Trainings,- Validierungs- und Testdatensätze, insbesondere um Diskriminierungen zu vermeiden, die im Artikel 10 erwähnt sind (Europäische Kommission, 2021, S. 55-56)
- Technische Dokumentation eines Hochrisiko-KI-Systems und seines Zwecks, die im Artikel 11 erwähnt ist (Europäische Kommission, 2021, S. 56-57)
- Aufzeichnungspflichten; Protokollierung und Dokumentation von Vorgängen und Ereignissen während des Betriebes, insbesondere um die Rückverfolgbarkeit von KI-Ergebnissen zu ermöglichen, die im Artikel 12 erwähnt sind (Europäische Kommission, 2021, S. 57)

- Transparenz und Bereitstellung von Informationen für die Nutzer, damit Nutzer die Resultate des Systems angemessen interpretieren und anwenden können, die im Artikel 13 erwähnt ist (Europäische Kommission, 2021, S. 57-58)
- Menschliche Aufsicht, um Risiken zu minimieren bzw. zu verhindern, die im Artikel 14 erwähnt ist (Europäische Kommission, 2021, S. 58-59)
- Angemessenes Mass an Genauigkeit, Robustheit und Cybersicherheit, die im Artikel 15 erwähnt ist (Europäische Kommission, 2021, S. 59-60).

Aus diesen Vorgaben kann man entnehmen, dass es hier um abstrakte technische Vorgaben geht, die einer weiteren Konkretisierung, Standards und Praxiseinsatz bedürfen. Es ist aus technischer Sicht zu prüfen, ob die hohen Anforderungen an Trainings-, Validierungs- und Testdatensätze fehlerfrei, repräsentativ, vollständig und relevant sind und überhaupt erfüllt werden können, die im Artikel 10 Abs. 3 erwähnt werden. Des Weiteren wird es beim Einsatz von KI-Systemen aus technischen Gründen schwierig sein, die im Verordnungsentwurf genannten hohen Anforderungen Transparenz und Rückverfolgbarkeit einzuhalten.

Der Verordnungsentwurf stellt eine grosse Bedeutung für den Einsatz der KI dar. Vor allem geht es dabei um eine Gratwanderung zwischen Innovationsförderung und Grundrechtschutz. Es sollen nicht nur potenzielle Risiken verhindert werden, sondern Innovationsanreize geschaffen werden. Im Grundsatz geht es aber auch darum, Vertrauen und Akzeptanz zu schaffen. Mit dem Einsatz von KI-Standards könnten die Grundätze und Anforderungen aus dem Verordnungsentwurf für die Praxis gut übersetzt und vollzogen werden.

## 5.2 Normungsroadmap DKE und DIN

Im Folgenden werden die Ergebnisse aus der "Deutschen Normungsroadmap" für künstliche Intelligenz, welche die Bedeutung von Standards im Bereich künstliche Intelligenz aufzeigt, erläutert.

Mit der genanntem Normungsroadmap stellt Deutschland weltweit als erstes Land eine vertiefte Analyse zum Bestand und des Bedarfs an internationalen Normen und Standards für KI vor. Für die Analyse wurde das Deutsche Institut für Normung (DIN) sowie die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (DKE) beauftragt.

Laut der Normungsroadmap DKE und DIN spielen Normen und Standards im Bereich künstliche Intelligenz eine besondere Rolle. Sie unterstützen den schnellen Transfer von Technologien aus der Forschung in die Anwendung und schaffen den Zugang zu internationalen Märkten für Unternehmen und ihre Innovationen. Durch die Festlegung von Anforderungen für Produkte, Dienstleistungen oder Prozesse gewährleisten Normen und Standards Interoperabilität und Qualität (Wahlster & Winterhalter, 2020, S. 4).

Die Normungsroadmap umfasst 70 Normungs- und Standardisierungsbedarfe und zeigt konkrete Potenziale auf. Aus den genannten Normungs- und Standardisierungsbedarfe stellt die Roadmap fünf übergreifende und zentrale Handlungsempfehlungen auf:

1. **Datenreferenzmodelle für Interoperabilität von KI-Systemen umsetzen:**

   In Wertschöpfungsketten agieren viele unterschiedliche Beteiligte zusammen, die verschiedene KI-Systeme haben. Damit diese KI-Systeme zusammen kommunizieren können, ist ein

Datenreferenzmodell erforderlich, um die Daten kompatibel, sicher, zuverlässig und flexibel auszutauschen. Standards für Datenreferenzmodelle aus unterschiedlichem Bereichen bilden die Grundlage für einen übergreifenden Datenaustausch und gewährleisten damit weltweit die Interoperabilität von KI-Systemen (Wahlster & Winterhalter, 2020, S. 4).

2. **Horizontale KI-Basis Sicherheitsnorm erstellen:**
   Systeme der künstlichen Intelligenz sind im Kern IT-Systeme. Für IT-Systeme existieren bereits viele Normen und Standards aus unterschiedlichen Anwendungsbereichen. Damit ein einheitliches Vorgehen beim Thema IT-Sicherheit von KI-Anwendungen gewährleistet wird, ist eine übergreifende "Umbrella-Norm" sinnvoll, die bereits existierende Normen und Prüfverfahren für IT-Systeme zusammenstellt und um KI-Aspekte erweitert. Diese Basis-Sicherheitsnorm kann dann durch Sub-Normen zu weiteren Themen erweitert werden (Wahlster & Winterhalter, 2020, S. 4).

3. **Praxisgerechte initiale Kritikalitätsprüfung von KI-Systemen ausgestalten:**
   Falls selbstlernende KI-Systeme über Menschen, deren Besitz oder Zugang zu knappen Ressourcen entscheiden, können demokratische Werte oder ungeplante Probleme in der KI individuelle Grundrechte in Gefahr setzen. Um KI-Systeme in ethisch unkritischen Anwendungsfeldern dennoch entwickeln zu lassen, sollten durch Normen und Standards eine initiale Kritikalitätsprüfung angelegt werden. Diese kann schnell und rechtssicher prüfen, ob ein KI-System solche Konflikte überhaupt verursachen kann (Wahlster & Winterhalter, 2020, S. 4).

4. **Nationales Umsetzungsprogramm "Trusted AI" zur Ertüchtigung der europäischen Qualitätsinfrastruktur initiieren und durchführen:**
   Bisher existieren keine verlässlichen Qualitätskriterien und Prüfverfahren für KI-Systeme. Dies ist eine Bedrohung für das wirtschaftliche Wachstum und die Wettbewerbsfähigkeit dieser Zukunftstechnologie. Es bedarf ein nationales Umsetzungsprogramm "Trusted AI", das die Grundlage für reproduzierbare und standardisierte Prüfverfahren legt, mit denen Eigenschaften von KI-Systemen wie Leistungsfähigkeit, Robustheit, Verlässlichkeit und funktionale Sicherheit geprüft und Aussagen über die Vertrauenswürdigkeit erzielt werden können. Normen und Standards definieren Anforderungen an diese und legen die Basis für die Zertifizierung und Konformitätsbewertung von KI-Systemen fest (Wahlster & Winterhalter, 2020, S. 5).

5. **Use Cases auf Normungsbedarf analysieren und bewerten:**
   Die Forschung im Bereich künstliche Intelligenz sowie industrielle Entwicklung und Anwendung von KI-Systemen sind hoch dynamisch. Aktuell existieren ganz viele Anwendungsfälle in den verschiedenen Einsatzfeldern der künstlichen Intelligenz. Aus den branchenrelevanten und anwendungstypischen Anwendungsfällen können sich Standardisierungsbedarfe für industriereife KI-Anwendungsfälle ableiten. Um Normen und Standards zu erarbeiten, ist es sinnvoll, wechselseitige Impulse aus Forschung, Industrie, Gesellschaft und Regulierung zu integrieren. Im Grundsatz dieses Ansatzes sollten die entwickelten Standards während dem Einsatz von Anwendungsfällen getestet und weiterentwickelt werden. Damit lassen sich der anwendungsspezifisch Bedarf vorzeitig erkennen und marktfähige Standards verwirklichen (Wahlster & Winterhalter, 2020, S. 5).

### 5.2.1 KI-Normen u. Standards: Smarte Assistenten für Behörden u. öffentliche Ämter

Im Rahmen der Ermittlung von Normungs- und Standardisierungsbedarf geht die Normungsroadmap KI auch auf die Anwendungsfälle im Bereich der öffentlichen Verwaltung ein. Daraus gehen folgende Punkte hervor:

Die demokratische Grundordnung bildet eine Stärke unserer Gesellschaft. Diese ist auf eine Vielzahl von historisch gewachsenen Behörden, Ämtern und Verwaltungsprozessen aufgebaut, die unsere Werte und Normen in die gelebte Praxis realisieren. Diese Überlegungen sollen nun für die Online-Welt aufgehen. In diesem Kontext werden smarte Assistenten entstehen, die auf der Grundlage von KI eine neue Form der Mensch-Maschine-Schnittstelle bzw. Bürger-Amt-Schnittstelle aufbauen. Smarte Assistenten können grosse Vorteile im Vergleich mit klassischen Ämtern haben: Bürgernahe, 24/7 Verfügbarkeit, einheitliche Qualität, Schnelligkeit, direkte Verarbeitung der digitalen Unterlagen, Automatisierung, Barrierefreiheit, Kosteneinsparungen, leichtere Bedienbarkeit für ältere Menschen und Menschen mit Behinderung. Solche Assistenten können am besten auf Grundlage von einheitlichen Standards entwickelt werden. Diese Anwendungsfälle werden auch die deutsche Sprache betreffen, was besonders hervorzuheben ist. Weshalb sollten zum Beispiel nicht alle öffentliche Ämter den gleichen KI-Standard haben, um einen Chatbot produktiv zu nutzen, welcher die Öffnungszeiten, Verantwortlichkeiten und Termine beschreibt? Hierbei leitet sich ein Handlungsbedarf ab (Wahlster & Winterhalter, 2020, S. 95).

## 5.3 Leitlinien "Künstliche Intelligenz" für Schweizerischen den Bund

Der Bundesrat hat im Jahr 2018 die "Künstliche Intelligenz" als zentrales Thema der Strategie Digitale Schweiz festlegt und eine departmentsübergreifende Arbeitsgruppe gebildet, die von dem Staatsekretariat für Bildung, Forschung und Innovation (SBFI) gesteuert wird. Die Arbeitsgruppe hat im 2019 einen Bericht zum Thema "Herausforderungen der Künstlichen Intelligenz" verfasst und auf dieser Basis die strategischen Leitlinien für den Umgang mit den Herausforderungen der künstlichen Intelligenz (KI) auf Ebene des Bundes erarbeitet. Diese Leitlinien dienen als allgemeiner Orientierungsrahmen für den Umgang mit KI in der Bundesverwaltung und sollen eine kohärente Politik sicherstellen, sowie eine Orientierung für die Bundesverwaltung und den Trägern von Verwaltungsaufgaben des Bundes in folgenden Bezugsrahmen geben:

- bei der Entwicklung sektoraler KI-Strategien mit dem Ziel, Kohärenz in der KI-relevanten Politik des Bundes zu erreichen; (SBFI, 2020, S. 2)
- bei der Einleitung oder Anpassung von spezifischen Regulierungen in allen sektoralen Anwendungsbereichen, die von KI betroffen sind; (SBFI, 2020, S. 2)
- bei der Erarbeitung und beim Einsatz von KI-Systemen in Arbeitsbereichen des Bundes; (SBFI, 2020, S. 2)
- bei der Mitarbeit des internationalen Regelwerks zu KI. (SBFI, 2020, S. 2)

In der Leitlinie werden für den Umgang mit KI als Grundlage die für die Schweiz geltende nationale und internationale Rechtsordnung, besonders die Bundesverfassung der Schweizerischen Eidgenossenschaft (BV, SR 101) und die Normen der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) definiert.

Die einzelnen Leitlinien enthalten folgende Aspekte:

Bei der ersten Leitlinie wird die Würde und das Wohl des einzelnen Menschen sowie das Gemeinwohl in Fokus gesetzt, insbesondere wird der **Schutz der Grundschutzrechte, das Verhindern der Diskriminierung, der Schutz der Privatsphäre sowie Datenschutzbestimmungen** als wichtige Vorgaben eingestuft (SBFI, 2020, S. 3).

Bei der zweiten Leitlinie geht es darum, dass der Bund bestmögliche Rahmenbedingungen für die Entwicklung und Anwendung der KI gewährleistet. Besonders wird bei dieser Leitlinie die technologieneutrale Regulierung, die einerseits die **Innovation** zulässt und andererseits **hohe Rechtssicherheit**, hervorgehoben (SBFI, 2020, S. 3-4).

Die dritte Leitlinie befasst sich mit der **Transparenz, Nachvollziehbarkeit und Erklärbarkeit**, welche als Grundvoraussetzungen für vertrauenswürdige KI beschrieben werden. Insbesondere wird bei dieser Leitlinie die Datenpolitik mit den Aspekten **hohe Datenqualität, Dokumentation** in den Fokus gesetzt. Des Weiteren wird die **zweckgebundene Erhebung und Verwendung von Daten** nach ethischen Standards sowie auch **die Sicherung der Interoperabilität der Datensysteme** als wichtig eingestuft (SBFI, 2020, S. 4-5).

Bei der vierten Leitlinie handelt es sich um die **Verantwortlichkeit**. Dabei wird beschrieben, dass beim Einsatz von KI die **Haftung** klar definiert werden muss (SBFI, 2020, S. 5).

Die fünfte Leitlinie beschreibt den Aspekt Sicherheit. Demnach müssen KI-Systeme sicher, robust und resilient konzipiert sein, um sich positiv auf die Menschen und die Umwelt auszuwirken und den Missbrauch oder Fehlanwendungen nicht zu begünstigen (SBFI, 2020, S. 5).

Die zwei letzten Leitlinien **Aktive Mitgestaltung der Gouvernanz von KI** und der **Einbezug aller relevanten nationalen und internationalen Akteure** beinhalten einerseits die aktive Mitgestaltung der globalen Gouvernanz von KI, besonders bei der Erarbeitung von Normen und Standards, und andererseits die Sicherstellung der Partizipation aller relevanten Anspruchsgruppen bei den politischen Entscheidungsprozessen (SBFI, 2020, S. 5).

Ähnlich wie beim Verordnungsentwurf der EU-Kommission für die künstliche Intelligenz geht es auch hier im Grundsatz darum. Vertrauen und Akzeptanz für KI-Systeme zu schaffen. Mit dem Einsatz von KI-Standards könnten die Grundätze und Anforderungen aus diesen Leitlinien für die Praxis gut übersetzt und vollzogen werden. Insbesondere können die Standards für die Leitlinien **Transparenz, Nachvollziehbarkeit und Erklärbarkeit** einen grossen Beitrag leisten, da diese Standards nebst einer gemeinsamen Sprache auch Methoden und Frameworks zur Verfügung stellen, womit man diese Kriterien erfüllen kann.

## 5.4 Künstliche Intelligenz und internationales Regelwerk–Bericht an den Bundesrat

Das EDA (Direktion für Völkerrecht DV) hat im Auftrag des Bundesrat vom 13.12.2019 in einem Bericht vom 13.04.2022 geprüft, wie internationale Regeln im KI-Bereich entstehen, wie sie zu qualifizieren sind und inwiefern dadurch Völkerrecht geschaffen wird, und ggf. Massnahmen unterbreiten, wie sich die Schweiz in diesem Kontext positionieren soll (Schweizerische Eidgenossenschaft, Eidgenössisches Department für auswärtige Angelegenheiten EDA, 2022).

Aus dem Bericht Künstliche Intelligenz und internationales Regelwerk vom 13.04.2022 werden folgende Vorschläge unterbreitet (Schweizerische Eidgenossenschaft, Eidgenössisches Department für auswärtige Angelegenheiten EDA, 2022):

1. Eine Fachgruppe zu Rechtsfragen wird geschaffen, welche als Anlaufstelle für rechtliche Expertise im Umgang mit KI in der Bundesverwaltung positioniert werden soll. Diese Fachgruppe soll den bereits bestehenden Strukturen zu KI des Kompetenznetzwerkes für künstliche Intelligenz CNAI und dem Administrativen Ausschuss der Plateforme Tripartite angegliedert werden. Mitglieder der Fachgruppe sollen nebst den Expertinnen und Experten aus den Bundesämtern auch die Expertinnen und Experten aus der Arbeitsgruppe "Recht und Technik" des EDA mit der Schweizerischen Akademie für technische Wissenschaften SATW sein. Diese Expertinnen und Experten können die Schweiz auch bei internationalen Prozessen unterstützen.
2. Der bestehende Administrativer Ausschuss Plateforme Tripartite in der Bundesverwaltung soll Positionen des Bundes sowie betroffenen Stellen in internationalen Gremien koordinieren. Damit sollte die Kohärenz der Schweizer Positionen zu KI bestärkt werden.
3. Die Zusammenarbeit mit den technischen Normierungsorganisationen soll gestärkt werden, die im internationalen Regelwerk zu KI Scharnierfunktion haben. Zu diesem Anlass soll das EDA zusammen mit der International Electrotechnical Commission IEC eine internationale Konferenz im Jahr 2022 in Genf organisieren, um das Zusammenspiel von technischen Standards, rechtlicher Regulierung im internationalen Regelwerk zu KI und Konformitätsbewertung zu behandeln und davon abgeleitet weitere Schritte zur Vertiefung über ein Instrument dieses Zusammenspiels zu finden.
4. Zur Aufnahme der Verhandlungen über ein Instrument des Europarats zu KI soll der Bundesrat der Schweizer Delegation bis Ende 2022 ein Mandat erteilen.

## 5.5 Beispiele und Quellen von KI-Standards

Mittlerweile existiert global eine Reihe von Standards im Bereich der künstlichen Intelligenz. Einige der KI-Standards, die für eCH von Bedeutung oder Grundlage für allfällige, eigene Standards sein könnten, werden wie folgt kurz beschrieben:

| Organisation | Standard | Beschreibung |
|---|---|---|
| ISO/IEC | ISO/IEC 23053™ - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) | Dieser Standard soll einen Rahmen für die Beschreibung von KI-Systemen bieten, die ML verwenden. Durch die Festlegung einer gemeinsamen Terminologie und eines gemeinsamen Konzepts für solche Systeme bietet dieses Dokument eine Grundlage für eine klare Erklärung der Systeme und verschiedener Überlegungen, die für ihre Konstruktion und ihre Verwendung gelten. |
| IEEE | IEEE P2941™ - Standard for Artificial Intelligence (AI) Model Representation, Compression, Distribution and Management | Dieser Standard definiert die KI-Entwicklungsschnittstelle, die interoperable Darstellung des KI-Modells, das Codierungsformat und das modellgekapselte Format für eine effiziente KI-Modellinferenz, -speicherung, -verteilung und -verwaltung |
| IEEE | IEEE P2975™ - Standard for Industrial Artificial Intelligence (AI) Data Attributes | Dieser Standard definiert Attribute in Bezug auf industrielle KI-Daten, die die Klassifizierung, Assoziation und Zuordnung zur Wertschöpfung mithilfe von Daten erleichtern. Zu den Attributen gehören unter anderem Datenquelle, Typ, Eigentum, Stichprobenhäufigkeit, Rückverfolgbarkeit, Datenschutzattribute für die Modellierung, Stichprobenziehung, Teilbarkeit und ihre Verwendung in KI-Algorithmen. |
| ISO/IEC | ISO/IEC 22989™ - Information technology — Artificial intelligence — Artificial intelligence concepts and terminology | Dieses Dokument bietet standardisierte Konzepte und Terminologie, um die Technologie der künstlichen Intelligenz besser zu verstehen |

Tabelle 1: Auszug KI-Standards (Quelle: Eigene Darstellung in Anlehnung an The Open Community for Ethics in Autonomous and Intelligent Systems [OCEANIS], n.d)

Um potenzielle Standards oder auch Standardisierungsinhalte und -prozesse zu identifizieren, analysieren, bewerten und eigene Aktivitäten darauf abzustimmen zu können, sollten Standardisierungsaktivitäten durch eCH o.ä. Organisationen systematisch beobachtet und gegebenfalls auch begleitet

werden. Hierfür können auch folgende insbesondere folgende Quellen in Anspruch genommen werden:

- Normungsorganisationen (DKE, DIN, ISO/IEC/ITU, CEN/CENELEC/ETSI)
- Standardisierung durch öffentliche Verwaltung anderer Staaten
- EU-Kommission
- Standardisierungsforen (z.B. IEEE, OMG, W3C, OASIS, IETF)

# 6 Beiträge von Experten und Organisationen

## 6.1 Hauptbeitrag Frauenhoferinstitut

### Über das Fraunhofer IAIS

Als Teil der grössten Organisation für anwendungsorientierte Forschung in Europa ist das Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS mit Sitz in Sankt Augustin bei Bonn eines der führenden Wissenschaftsinstitute auf den Gebieten Künstliche Intelligenz, Maschinelles Lernen und Big Data in Deutschland und Europa. Mit seinen mehr als 300 Mitarbeitenden unterstützt das Institut Unternehmen bei der Optimierung von Produkten, Dienstleistungen, Prozessen und Strukturen sowie bei der Entwicklung neuer digitaler Geschäftsmodelle. Damit gestaltet das Fraunhofer IAIS die digitale Transformation unserer Arbeits- und Lebenswelt. Ein wichtiges Schwerpunkt-Thema des Fraunhofer IAIS stellt die Vertrauenswürdigkeit und Zuverlässigkeit im Kontext von KI-Systemen dar.

### Über den Autor

Dr. Maximilian Poretschkin leitet das Team „KI-Absicherung und -Zertifizierung“ am Fraunhofer IAIS und verantwortet dort die Aktivitäten im Bereich Absicherung, Prüfung und Standardisierung von KI-Anwendungen. In dieser Funktion hat er bereits eine Vielzahl an Projekten mit Forschungspartnern, Industriekunden und der öffentlichen Hand durchgeführt. Er leitet zudem ZERTIFIZIERTE KI, das erste Umsetzungsprojekt der deutschen Normungsroadmap KI, in welchem das Fraunhofer IAIS, das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Deutsche Institut für Normung (DIN) sowie weitere Forschungspartner Prüfverfahren für die Zertifizierung von KI-Systemen entwickeln. Darüber hinaus ist er Leiter der Arbeitsgruppe „Prüfung und Zertifizierung“ der Normungsroadmap KI und Mitglied des Normenausschusses NA 043-01-42 AA „Künstliche Intelligenz“ beim Deutschen Institut für Normung (DIN).

### Einleitung und Motivation

Der Verein eCH fördert, entwickelt und verabschiedet Standards im Bereich E-Government und ist damit Teil der Schweizer E-Government Strategie. Künstliche Intelligenz hat ein grosses Potenzial für den Einsatz in der öffentlichen Verwaltung. Zu denken sind hier etwa an Sprachassistenten und Bots in der G2C-Schnittstelle oder die KI-basierte Automatisierung von Verwaltungsvorgängen (z. B. die Bearbeitung von Steuererklärungen). Darüber hinaus können KI-Anwendungen auch für weitere hoheitliche Aufgaben zum Einsatz kommen, wie z. B. zur Schwarzarbeitkontrolle oder im Bereich des Predictive Policing. Zentrale Erfolgsfaktoren für die systematische Einführung entsprechender KI-Anwendungen in der öffentlichen Verwaltung – aber auch in anderen Kontexten – stellen Interoperabilität und Qualitätssicherung dar. Ein bewährter Weg, diesen Anforderungen Genüge zu tragen, stellen Standards und Normen dar. Die aktive Mitgestaltung von nationalen und internationalen Standards ist ebenfalls eine Forderung der Leitlinien „Künstliche Intelligenz“ (Schweizerische Eidgenossenschaft 2020), welche vom Schweizer Bundesrat im November 2020 für die Bundesverwaltung verabschiedet worden sind. Der vorliegende Artikel analysiert daher das Potenzial entsprechender KI-Standards für den Einsatz in der öffentlichen Verwaltung. Er wird durch eCH vorgegebene Fragen strukturiert.

**Allgemeine Überlegungen zu KI-Standards**

KI-Anwendungen kommen bereits heute an vielen Stellen unseres Lebens zum Einsatz, etwa bei einer KI-basierten Qualitätskontrolle im industriellen Umfeld, in Assistenzsystemen, welche Radiologen bei der Auswertung medizinischer Bilder unterstützen, in Kreditvergabesysteme oder perspektivisch beim autonomen Fahren. Diese Beispiele zeigen überdeutlich auf, dass das volle Potenzial nur dann realisiert werden kann, wenn der Einsatz von Künstlicher Intelligenz nach hohen Qualitätsmassstäben erfolgt. Hierbei können Standards ein erprobter Weg sein, um entsprechende Massstäbe zu definieren.

**Anforderungen an die Qualität von KI-Anwendungen**

Im Wesentlichen können die Qualitätsmassstäbe für KI-Anwendungen in zwei Bereiche untergliedert werden: Der erste Bereich umfasst die Vertrauenswürdigkeit von Künstlicher Intelligenz. Bereits 2018 hat die High-Level Expert Group on AI der Europäischen Kommission Empfehlungen (High-Level Expert Group on Artificial Intelligence 2018) veröffentlicht, welche die Anforderungen an die Vertrauenswürdigkeit von Künstlicher Intelligenz definieren. Hierzu gehören insbesondere:

- die Vermeidung von ungerechtfertigter Diskriminierung,
- eine angemessene Aufteilung der Verantwortung zwischen Mensch und KI-Anwendung sowie eine angemessene Gestaltung der Mensch-Maschine Schnittstelle,
- Anforderungen an die Transparenz, Nachvollziehbarkeit und Wirkweise der KI-Anwendungen,
- Anforderungen an die technische Robustheit und Sicherheit (sowohl im Sinne von funktionaler als auch IT-Sicherheit (safety & security)),
- die Sicherstellung entsprechender Rechenschaftspflichten,
- Wahrung des Datenschutzes und Datenqualitätsmanagement,
- Anforderungen, die sich aus dem gesellschaftlichen und ökologischen Wohlergehen ergeben.

Diese Anforderungen werden auch von den Leitlinien „Künstliche Intelligenz“ für den Bund des Schweizer Bundesrates (Schweizerische Eidgenossenschaft 2020) aufgegriffen, welche noch einmal betonen, dass der Mensch im Zentrum der Anwendung von Künstlicher Intelligenz stehen muss. Für eine umfassende wissenschaftliche Behandlung und Übersicht von unterschiedlichen nationalen und internationalen Leitlinien für den Einsatz von Künstlicher Intelligenz siehe auch (Jobin 2019).

Der zweite Bereich umfasst die Sicherstellung der Interoperabilität von KI-Systemen, insbesondere die Schaffung entsprechender Datenreferenzmodelle, welche notwendig sind, um Daten sicher, zuverlässig, flexibel und kompatibel auszutauschen.

**Produkt- und Prozessstandards**

In Anlehnung an Best Practices in der Softwareentwicklung können zwei wichtige Klassen bei den benötigten Standards identifiziert werden: Produkt- und Prozessstandards. Produktstandards legen konkrete Anforderungen an bestimmte KI-Anwendungen oder Teilsysteme von ihnen fest bzw. formulieren Kriterien, welche Beurteilung der Qualität der KI-Anwendungen ermöglichen. Prozessstandards legen anerkannte Arbeitsabläufe zur Entwicklung oder dem Betrieb von KI-Anwendungen fest und haben zum Ziel, die Qualität der KI-Anwendung indirekt über die Qualität des Entwicklungsprozesses zu verbessern. Allgemein ist zu erwarten, dass beide Sorten Standards im Bereich des eGovernment von Bedeutung sind. Darüber hinaus gibt es weitere Sonderfälle, für welche ebenfalls Standards benötigt werden. Hierzu gehören beispielsweise KI-Dienstleistungen, Anforderungen, welche an die Qualifizierung bestimmter Personengruppen (etwa KI-Entwickler*innen, KI-Nutzer*innen, KI-Prüfer*innen) im Umgang

mit Künstlicher Intelligenz zu stellen sind oder KI-Managementsysteme. Managementsysteme bieten einen bewährten Zugang, um Strukturen zu beschreiben, mit Hilfe derer Organisationen bestimmte Ziele durch geeignete technisch-organisatorische Massnahmen umsetzen können. Solche Managementsysteme haben sich für einige Fragestellungen als extrem erfolgreich erwiesen, wie etwa im Bereich der Qualitätssicherung (ISO 9000 Reihe) oder der Informationssicherheit (ISO 27000 Reihe). Aktuell wird von der ISO ein Standard für KI-Managementsysteme (ISO/IEC CD 42001 Information Technology — Artificial intelligence — Management system) entwickelt[1], welcher für alle Organisationen, die KI einsetzen von Bedeutung sein wird.

**Analyse der Fragestellungen von eCH**

1) **Welche Potential besteht für die Einführung von KI-Standards?**

Das Deutsche Institut für Normung (DIN) hat zusammen mit dem Verband der Elektrotechnik Elektronik Informationstechnik e. V. (VDE) im Dezember 2020 die weltweit erste Normungsroadmap (Winterhalter 2020) im Bereich KI veröffentlicht. Dieses Dokument bietet eine internationale Bestandsaufnahme an bestehenden Standards und Normen im Bereich Künstliche Intelligenz und zeigt darüber hinaus zahlreiche Bedarfe für weitere Standards und Normen auf. Dabei wird auch der Bereich der öffentlichen Verwaltung als expliziter Handlungsbedarf formuliert. Auch die Schweizer Bundesverwaltung zeigt ein grosses Potenzial für KI-Anwendungen auf (Braun Binder 2021).

2) **Ist ein relevanter Nutzen mit der Einführung von neuen KI-Standards zu erwarten?**

Der volkswirtschaftliche Nutzen durch die Verwendung von Normen wird allein in Deutschland auf 17 Mrd. € geschätzt. Angesichts der mannigfaltigen Anwendungsmöglichkeiten für KI-Systeme einerseits und des disruptiven Veränderungspotenzials andererseits, welches dafür sorgt, dass viele analoge Systeme durch KI-Systeme ersetzt werden, ist davon auszugehen, dass KI-Standards und -Normen im Speziellen ebenfalls einen signifikanten volkswirtschaftlichen Nutzen haben werden. Zudem ist abzusehen, dass harmonisierte Europäische Normen eine zentrale Rolle für die Umsetzung des Artificial Intelligence Act (European Commission 2021) spielen werden, welcher mindestens insofern für die Schweiz relevant sein wird, als dass die Regulierung ebenfalls Systeme betrifft, die in einem Drittland betrieben werden, sofern ihr Output in der Europäischen Union zur Anwendung kommt.

3) **Gibt es bereits internationale Standards (oder de facto Standards) und in welchen Bereichen werden Sie bereits eingesetzt?**

Es gibt bereits eine Reihe an nationalen und internationalen Standards, viele weitere sind in Erarbeitung. Einen guten Überblick hierzu gibt die Normungsroadmap KI (Winterhalter 2020). Hervorzuheben sind: Standards zu Grundlagen und zur Terminologie von KI-Systemen (z. B. ISO/IEC TR 24028, ETSI GR ENI 004, ETSI GR NFV 003), Standards zum Lebenszyklus von KI-Systemen (z. B. DIN SPEC 92001-1, DIN SPEC 92001-2) sowie für bestimmte Domänen, wie etwa KI-basierte Bilderkennung (z. B. DIN SPEC 13266). Ferner gibt es eine Normenreihe (ISO/IEC TR 20547-1,5) für Big Data,

[1] Für einen Überblick zu dem entstehenden Standard und insbesondere einen Vergleich mit dem Regulierungsvorschlag der EU-Kommission siehe die Fraunhofer-Studie (Mock 2021).

welche Begrifflichkeiten und Referenzarchitekturen festlegt sowie für Datenqualität (z. B. ISO/IEC 25012).

4) **Welche Form von KI-Standards zu welchen Themen stehen dabei im Vordergrund? (Datenaustausch-, Dokumenten-, Formate-, Methoden-, Architektur-Standards etc.)**

Wie unter 3) dargelegt, stehen aktuell die Terminologie, Vorgaben zum Lebenszyklus von KI-Systemen sowie an die Datenqualität im Fokus. Dies wird durch zahlreiche laufende Standardisierungsaktivitäten ergänzt, etwa auf internationaler Ebene im ISO/IEC JTC 1/SC 42 “Artificial Intelligence” zu den Themen Terminologie, Datenqualität, Risikomanagement, Anwendungshilfen, Metriken und Aspekte von KI-Organisationen.

5) **Sind Stakeholder mit hohem Interesse an der Einführung von KI-Standards identifizierbar? Welche Stakeholder sind das?**

Angesichts des enormen Anwendungspotenzials von KI-Anwendungen gibt es eine Vielzahl potenzieller Stakeholder. Zum einen sind hier die Entwickler*innen und Betreiber*innen von KI-Anwendungen zu nennen, die auf klare Qualitätsanforderungen und Standards angewiesen sind, welche die Interoperabilität sicherstellen. Daneben haben Nutzer*innen und Betroffene ebenfalls ein grosses Interesse an (nachprüfbaren) Qualitätsstandards. Da Künstliche Intelligenz im Rahmen der öffentlichen Verwaltung auch in sensiblen Bereichen zum Einsatz kommen kann, ist grundsätzlich von einem allgemein hohen Interesse an entsprechenden Standards auszugehen. Dies belegt auch das gemeinsame Weissbuch (Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway and the UK 2020) der Europäischen Rechnungshöfe, welches ein Vorgehen zur Prüfung[2] der Ordnungsmässigkeit und Wirtschaftlichkeit von KI-Anwendungen in der Verwaltung vorschlägt, was ebenfalls die Bedeutung von Standards als Manifestation entsprechender Qualitätsmassstäbe unterstreicht.

6) **Reichen bereits vorhandenen KI-Standards aus? Ist die Ergänzung bzw. die Einführung weiterer Standards grundsätzlich sinnvoll bzw. verspricht sie einen massgeblichen Nutzen versprechen?**

Die bereits angesprochenen Standards bilden eine wichtige Grundlage für den Einsatz von KI-Systemen, reichen bei weitem aber nicht aus, wie die Bedarfsanalyse der Normungsroadmap KI (Winterhalter 2020) zeigt. Zahlreiche laufende weltweite Standardisierungsaktivitäten sind ebenfalls ein eindrucksvoller Beleg des Bedarfs. Eine Analyse der aktuell entstehenden Standards zeigt, dass insbesondere in Bezug auf spezifische Anforderungen für den Einsatz von Systemen innerhalb der öffentlichen Verwaltung noch ein erheblicher Handlungsbedarf besteht.

7) **Welche Organisationen oder Personen könnten national die Entwicklung entsprechender KI-Standards vorantreiben?**

Allgemein sollte die Entwicklung entsprechender KI-Standards durch interdisziplinär besetzte Expert*innengremien vorangetrieben werden, welche KI- und Domänenexpertise aufweisen und Vertreter von Entwickler*innen, Betreiber*innen, Nutzer*innen und Betroffenen sowie entsprechender Aufsichtsbehörden umfassen. Für Standards, welche allgemeine Qualitätsanforderungen für KI-Systeme betreffen, sollte eCH sich an internationalen Standardisierungsaktivitäten beteiligen (ggf. über Obmänner in den Spiegelgremien der SNV). Die aktive Mitgestaltung internationaler KI-Standards und Normen ist

[2] Vergleiche auch den KI-Prüfkatalog (Poretschkin 2021).

auch eine Kernforderung der Leitlinien „Künstliche Intelligenz“ für den Bund (Schweizerische Eidgenossenschaft 2020). Daneben sollte eCH für spezifische Anforderungen an KI-Anwendungen innerhalb der Schweizer Verwaltung eigene Standardisierungsaktivitäten erwägen, beispielsweise für die Erhebung von Nutzer*innenanforderungen, welche von KI-Anwendungen in dieser Domäne einzuhalten sind.

**8) Wie werden die Chancen für die erfolgreiche Erarbeitung von KI-Standards eingeschätzt?**

Die eingangs erwähnten Beispiele zeigen, dass Standards für KI-Anwendungen erfolgreich umgesetzt werden können. Angesichts der Vielzahl der möglichen Anwendungsfälle sollte eine sinnvolle Priorisierung vorgenommen werden, da für die Erarbeitung solcher Standards angemessene Ressourcen bereitgestellt werden müssen. Insbesondere sollte die Erarbeitung anhand konkreter Anwendungsfälle unter Einbeziehung entsprechender Branchen- und technischer Expert*innen vorgenommen werden.

**9) Wie kann man bei der Erarbeitung von neuen KI-Standards vorgehen?**

KI-Systeme unterscheiden sich in vielerlei Hinsicht von herkömmlichen IT- Systemen und Software, da sie beispielsweise nicht modular durchgetestet werden können und unter Umständen im Betrieb weiterlernen können. Entsprechende Standards für KI-Systeme sollten daher immer anhand konkreter Use Cases entwickelt und getestet werden und innerhalb eines kontinuierlichen Verbesserungsprozesses regelmässig angepasst werden. Da KI-Anwendungen in einer Vielzahl von Domänen zum Einsatz kommen, kommen für diese auch eine Vielzahl bestehender Gesetzesvorschriften sowie bestehender Standards und Normen zum Einsatz. Bei der Formulierung von neuen KI-Standards ist daher insbesondere darauf zu achten, dass diese kompatibel mit bestehenden Anforderungen (etwa aus dem Bereich Softwareentwicklung, IT-Sicherheit, etc.) sind. Umgekehrt kann es notwendig sein, bestehende Standards auf ihre „KI-Tauglichkeit“ zu testen, wie es beispielsweise die KI-Strategie der deutschen Bundesregierung (Bundesministerium für Wirtschaft und Energie 2018) fordert.

**10) Was sind die Chancen entsprechender KI-Standards in der Schweiz? Inwieweit ist die Machbarkeit gewährleistet? (Möglich im internationalen Kontext? Möglich im Rahmen von spezifischen Phasen?)**

Angesichts mannigfaltiger Anwendungsmöglichkeiten für KI-Anwendungen innerhalb der öffentlichen Verwaltung ist davon auszugehen, dass KI-Standards ein grosses Potenzial für Anwendungen in der öffentlichen Schweizer Verwaltung haben werden. Hierbei sollte geprüft werden, an welchen Stellen internationale Standards adaptiert werden können und wo spezifische nationale Lösungen benötigt werden.

**11) Sollten KI-Standards in bestimmten Felder angestrebt werden? Welche Schlussfolgerungen ergeben sich für eGovernment bzw. auch für eCH?**

Eine Analyse des Einsatzes von Künstlicher Intelligenz innerhalb der Schweizer Verwaltung (Braun Binder 2021) identifiziert aus vertikal-sektoraler Sicht insbesondere KI-Potenziale im Bereich der Steuer- und Sozialverwaltung, bei der Arbeit von Polizei und Justiz sowie für Chatbots an der G2C-Schnittstelle. Horizontale Themen, für die entsprechende Standards benötigt werden, stellen Fairness und Nichtdiskriminierung, Gestaltung der Mensch-Maschine Schnittstelle, Transparenz und Nachvollziehbarkeit, Verlässlichkeit und Robustheit, Sicherheit sowie Datenschutz dar.

Aus Perspektive des eGovernments sind wichtige Motivatoren für die Formulierung entsprechender KI-

Standards die Interoperabilität unterschiedlicher Systeme, die Formulierung klarer Qualitätskriterien bei der Etablierung entsprechender KI-Anwendungen (insbesondere für die Fälle des Ankaufs externer Lösungen oder für die Steuerung und Überwachung entsprechender Dienstleister) sowie die notwendigen Grundlagen für einen revisionssicheren Betrieb der Systeme.

eCH sollte in Konsequenz internationale Standardisierungsaktivitäten begleiten und verfolgen und wo notwendig, etwaige „KI-Standardisierungslücken" für Use Cases innerhalb der Schweizer Bundesverwaltung durch eigene Standardisierungsaktivitäten schliessen.

**Literaturverzeichnis**

Braun Binder, et al. „Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen." Basel, 2021.

Bundesministerium für Wirtschaft und Energie. „Strategie Künstliche Intelligenz der Bundesregierung." Berlin, 2018.

European Commission. „Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts." Brüssel, 2021.

High-Level Expert Group on Artificial Intelligence. „Ethics Guidelines for Trustworthy AI." Brüssel, 2018.

High-Level Expert Group on Artificial Intelligence. „The Assessment List for Trustworthy Artificial Intelligence for self assessment." Brüssel, 2019.

Jobin, et al. „The global landscape of ethics guidelines." *Nature Machine Intelligence*, 2019.

Mock, et al. „Management System Support for Trustworthy Artificial Intelligence." Sankt Augustin, 2021.

Poretschkin, et al. „Leitfaden zur Gestaltung vertrauenswürdiger Künstlicher Intelligenz - KI-Prüfkatalog." Sankt Augustin, 2021.

Schweizerische Eidgenossenschaft, der Bundesrat. „Leitlinien Künstliche Intelligenz." 2020.

Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway and the UK. „Auditing machine learning algorithms - A white paper for public auditors." 2020.

Winterhalter, Wahlster, et al. „Deutsche Normungsroadmap Künstliche Intelligenz." Berlin, 2020.

## 6.2 Beitrag Bundesamt für Kommunikation "BAKOM"

Im Rahmen der Potenzialanalyse wurden die folgenden Fragenstellungen auch an das Bundesamt für Kommunikation gestellt. BAKOM stellt folgende Überlegungen zum Thema Standards im Bereich der künstlichen Intelligenz dar, die in Form eines Interviews verfasst worden sind.

1) **Sind Standards für Künstliche Intelligenz ein Thema bei BAKOM? Wenn ja, welche Aktivitäten gibt es in diesem Bereich?**

   KI-Standards sind ein wichtiges Anliegen des BAKOM, das ihre Entwicklung durch nationale und internationale Initiativen unterstützt.

   Auf nationaler Ebene beteiligte sich das BAKOM an der Entwicklung von Richtlinien für den Umgang mit KI-Herausforderungen auf Bundesebene. Diese sieben Leitlinien fordern den Bund auf, den Menschen in den Mittelpunkt von KI-Systemen zu stellen, förderliche Rahmenbedingungen für die Entwicklung und den Einsatz von KI zu gewährleisten, Transparenz, Nachvollziehbarkeit, Verantwortung, Sicherheit und Nachvollziehbarkeit zu fördern und schliesslich die aktive Teilnahme an globaler KI-Governance zu unterstützen. Zudem hat das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) in seinem Bericht an den Bundesrat vom 17. November 2021 aufgezeigt, wie KI-basierte Kommunikationsintermediäre und -plattformen die öffentliche Kommunikation in der Schweiz und die Meinungsbildung der Schweizer Bevölkerung beeinflussen, und der Bundesrat hat das UVEK beauftragt, ihm bis Ende 2022 in einer Diskussionsnotiz mitzuteilen, ob und wie Kommunikationsplattformen reguliert werden sollen.

   Auf internationaler Ebene spielt das BAKOM eine aktive Rolle bei der Gestaltung der globalen Governance von KI und beteiligt sich an zahlreichen Standardsetzungsprozessen innerhalb des Europarates, der OECD, der UNESCO und der ITU. Das BAKOM verfolgt den Fortgang der Arbeiten an den Verordnungsentwürfen zur KI in der Europäischen Union (EU).

   Technische Standards im Zusammenhang mit künstlicher Intelligenz existieren auf EU-Ebene noch nicht, aber das BAKOM verfolgt aufmerksam die Aktivitäten der europäischen Standardisierungsorganisationen (ESO) – CEN, CENELEC und ETSI, ohne sich (zumindest vorerst) an der Entwicklung dieser Standards zu beteiligen. Dennoch ist hervorzuheben, dass sich die Normungsarbeit der ESOs derzeit in einer Definitions- und Organisationsphase befindet.

2) **Sieht BAKOM ein Handlungsbedarf im Bereich KI-Standards? Wenn ja, welchen Nutzen sieht BAKOM beim Einsatz von KI-Standards?**

   BAKOM erachtet es als wichtig, sowohl die Chancen als auch die Risiken von KI zu erkennen und wird 2022 ein erstes Follow-up der Richtlinien durchführen. Das BAKOM und die Schweiz plädieren generell für einen liberalen Ansatz im Bereich der KI-Standards; keine „Über"-Regulierung, sondern Berücksichtigung bestehender Werte und Standards, insbesondere im Hinblick auf Menschenrechte.

Robuste und vollständige technische Standards sind unerlässlich, um die technische Übereinstimmung von Lösungen mit dem zum Zeitpunkt ihres Inverkehrbringens geltenden Rechtsrahmen zu gewährleisten. Als Regulator kann das BAKOM diese Standards verwenden, um verbindliche Anforderungen festzulegen, oder die Standards auf freiwilliger Basis verwenden, um eine Konformitätsvermutung mit bestimmten Anforderungen zu begründen.

**3) Welche Form von KI-Standards zu welchen Themen stehen dabei im Vordergrund? (Datenaustausch-, Dokumenten-, Formate-, Methoden-, Architektur-Standards etc.)**

Die KI-Richtlinien konzentrieren sich auf sieben Themen:

i: Menschenzentriert: Die Würde und das Wohl jedes Einzelnen sowie das öffentliche Interesse müssen bei der Entwicklung und Nutzung von KI-Systemen im Vordergrund stehen.

ii. Förderbedingungen für die Entwicklung und Nutzung von KI: Sicherstellung günstiger Bedingungen für die Entwicklung von KI und Positionierung der Schweiz als einer der Hauptstandorte für Forschung, Anwendung und kommerzielle Nutzung von KI.

iii. Transparenz, Nachvollziehbarkeit und Erklärbarkeit: KI-basierte Entscheidungsprozesse müssen identifizierbar und überprüfbar gestaltet werden.

iv. Haftung: Um Verantwortlichkeiten bei Schäden, Unfällen oder Rechtsverstössen festzulegen, ist es notwendig, die Haftung beim Einsatz von KI eindeutig festzulegen.

v. Sicherheit: KI-Systeme müssen von ihrem Design her sicher, robust und belastbar sein, damit sie positive Wirkungen entfalten können und nicht missbraucht oder zweckentfremdet werden können.

vi. Aktive Beteiligung an der KI-Governance: Für die Schweiz ist es unabdingbar, sich aktiv an der globalen Governance im Bereich der KI zu beteiligen und sich an der Entwicklung internationaler Normen und Standards im Bereich der KI zu beteiligen. KI unter Wahrung der eigenen Interessen und Werte.

vii. Einbezug aller relevanten Akteure auf nationaler und internationaler Ebene: Die Schweiz muss sich dafür einsetzen, dass Entscheidungsprozesse zur KI-Governance alle Anspruchsgruppen einbeziehen.

Es muss auch berücksichtigt werden, dass die von den europäischen Normungsorganisationen erstellten technischen Normen mit allgemeinem Charakter fortgeschrittene Kenntnisse auf diesem Gebiet beinhalten und es den Herstellern ermöglichen, Qualitätsprodukte herzustellen. Von der Europäischen Kommission in Auftrag gegebene harmonisierte Normen gewährleisten die Konformitätsvermutung von Produkten, die auf den Markt gebracht werden.

**4) Was sind die Chancen entsprechender KI-Standards in der Schweiz? Inwieweit ist die Machbarkeit gewährleistet?**

In der Schweiz bleibt die Regulierung von «intelligenter» KI und die Schaffung entsprechender

Standards eine Herausforderung: Es gilt, die Balance zwischen «Förderung von Innovationen» und «Risikominderung» zu finden. Dazu müssten verbindliche und unverbindliche Regulierungsinstrumente kombiniert werden. Die Einbindung aller Akteure und Interdisziplinarität sind notwendig, ebenso wie eine öffentliche Debatte, um die Bevölkerung über die Herausforderungen und Chancen von KI aufzuklären.

Um die Umsetzbarkeit dieser Standards zu gewährleisten, ist es auch wichtig, die grenzüberschreitende Zusammenarbeit mit der Europäischen Union sowie den anderen internationalen Partnern der Schweiz zu fördern. Tatsächlich wird die Entwicklung und Einführung internationaler KI-Standards effektive und zuverlässige Lösungen ermöglichen, die das Vertrauen von Verbrauchern, Unternehmen und Regulierungsbehörden stärken.

Das BAKOM hält es für illusorisch, Schweizer KI-technische Standards entwickeln zu wollen. Damit diese Normen einen gewissen Geltungsbereich haben können, muss eine Normung auf internationaler Ebene erfolgen. Zudem ist das nötige Fachwissen in der Schweiz nicht unbedingt vorhanden.

Von der Europäischen Kommission (EK) in Auftrag gegebene harmonisierte technische Normen können als Referenzen in die Schweizer Gesetzgebung aufgenommen werden. Dies ist z. B. im Bereich der Telekommunikation bereits der Fall.

**5) Sollten KI-Standards in bestimmten Felder angestrebt werden? Welche Anwendungsfälle ergeben sich für eGovernment?**

Besonderes Augenmerk sollte auf die Risiken der Diskriminierung beim Einsatz von KI im öffentlichen Sektor gelegt werden, sei es zur Entwicklung von Rechtsnormen oder zur Rechtsanwendung. Dies kann eine Risikoanalyse während des Entwurfs der Systeme und eine regelmässige Überwachung und Bewertung umfassen. Dazu ist es notwendig, sich auf bestehende Regeln und Standards zu stützen, beispielsweise in Bezug auf Menschenrechte, Datenschutz und soziale Verantwortung.

Für technische Standards ist es wahrscheinlich ratsam, dem Ansatz auf der Grundlage des Risikoniveaus im Entwurf der EG-Verordnung zu folgen.

## 6.3 Beitrag Kompetenznetzwerk KI (CNAI) Bund

Im Rahmen der Potenzialanalyse wurde auch ein Beitrag des Kompetenznetzwerks für künstliche Intelligenz (CNAI: Competence Network for Artificial Intelligence / Kompetenznetzwerk für KI) verfasst. Die folgenden Fragenstellungen sind auch an das Kompetenznetzwerk für künstliche Intelligenz (CNAI) gestellt. Diego Kuonen, Leiter ad interim der Geschäftsstelle des Kompetenznetzwerks für künstliche Intelligenz stellt folgende Überlegungen zum Thema Standards im Bereich künstliche Intelligenz dar, die in Form eines Interviews verfasst worden sind.

1) **Sind Standards im Bereich Künstliche Intelligenz ein Thema beim Kompetenznetzwerk? Wenn ja, welche Aktivitäten gibt es in diesem Zusammenhang direkt oder indirekt?**

   Beim Kompetenznetzwerks für künstliche Intelligenz (CNAI: Competence Network for Artificial Intelligence / Kompetenznetzwerk für KI) erarbeiten wir Grundlagen, um den Einsatz von und das Vertrauen in künstliche Intelligenz (KI) und andere neue Technologien innerhalb der Bundesverwaltung nachhaltig zu fördern. Das CNAI leistet ausserdem einen Beitrag zur Information der Öffentlichkeit. Es trägt mit seiner Projektübersicht zur Transparenz der laufenden KI-Projekte in der Bundesverwaltung (und darüber hinaus) bei.

   Das CNAI erarbeitet keine Standards, jedoch hat das CNAI eine einheitliche KI-Terminologie entwickelt. Die Einführung einer einheitlichen Terminologie ist ein zentraler Grundstein für die Funktionen des CNAI. Eine gemeinsame Sprache und ein entsprechendes gemeinsames Begriffsverständnis auf Ebene der Bundesverwaltung erleichtert den aktiven Erfahrungs- und Wissensaustausch innerhalb des Netzwerks CNAI und darüber hinaus. Darüber hinaus gibt es auch auf der Webseite von CNAI (CNAI.swiss) eine Projektdatenbank sowie eine Liste von KI-relevanten Projekten in der Bundesverwaltung. Die in diesen Projekten beschriebenen Anwendungsfälle lehnen sich auch an einzelne Standards, die auch in Projekten eingesetzt werden könnten.

   Des Weiteren werden im CNAI zwei Communities («Community of Practice», «Community of Expertise») aufgebaut, die Synergien mit der bestehenden Community «Data Science for Public Good» des Kompetenzzentrums für Datenwissenschaft (DSCC: Data Science Competence Center) und dessen «Expertinnen- und Experten-Pool DSCC» nutzt.

2) **Welchen Nutzen sehen Sie beim Einsatz von KI-Standards für den Bund oder für die Öffentlichkeit?**

   Mit KI- Standards können eine gemeinsame Sprache geschaffen werden und damit Probleme und Risiken gemeinsam gelöst werden. Damit kann auch die Vertrauenswürdigkeit für KI-Systeme geschaffen werden und die Interoperabilität sichergestellt werden.

**3) Welche Form von KI-Standards zu welchen Themen stehen dabei im Vordergrund? (Datenaustausch-, Dokumenten-, Formate-, Methoden-, Architektur-Standards etc.)**

Im Fokus sollten zuerst Terminologie und Regelwerk für die Anwendung von KI-Systemen stehen. Diese sind die wichtigsten Grundlagen für die Standardisierung im Bereich KI.

**4) Was sind die Chancen entsprechender KI-Standards in der Schweiz? Inwieweit ist die Machbarkeit gewährleistet?**

KI-Standards können auch als Enabler für die KI-Technologien betrachtet werden. Damit kann einerseits die Vertrauenswürdigkeit gefördert werden und andererseits auch Qualität für die Daten und Methoden sichergestellt werden. Damit werden auch Werte geschaffen, um allfällige Risiken zu vermeiden.

Aktuell arbeiten Bundesstellen an normativen Vorgaben, um Voraussetzungen für Standards und Normen zu schaffen. In nächster Zeit wird ein Bericht an den Bundesrat vorgestellt, worin die weitere Vorgehensweise im internationalen Kontext im Zusammenhang mit KI und deren Rahmenbedingungen definiert werden.

Für die Standardisierung und Normierung sollten auch eine Zusammenarbeit mit internationalen Organisationen erfolgen. Die Machbarkeit bzw. die Anwendung der KI-Standards können nur ermöglicht werden, wenn die Grundlagen dafür geschaffen sind.

**5) Sollten KI-Standards in bestimmten Felder angestrebt werden? Welche Anwendungsfälle ergeben sich für eGovernment?**

Die Frage kann nicht abschliessend beantwortet werden. Es gibt eine Reihe von Anwendungsfällen. Auf der Webseite von CNAI gibt es eine Projektdatenbank, worin einige KI-Anwendungsfälle der Bundesverwaltung aufgezeigt werden. Die KI-Standards könnten punktuell auch aus diesen Anwendungsfällen abgeleitet werden.

Für die weitere Behandlung dieses Thema könnte sich Diego Kuonen vorstellen, dass innerhalb vom CNAI ein Knoten «KI-Standards» geschaffen wird, in welchem eCH den Lead für KI-Standardisierungen im Bereich E-Government in der Schweiz übernimmt.

# 7 Schlussfolgerungen für eCH

Die Analyse der Studien, Berichte und der Beiträge in dieser Arbeit zeigen, dass die Erarbeitung und der Einsatz von Standards im Bereich künstlicher Intelligenz für die öffentliche Verwaltung in der Schweiz von grossem Interesse sind. Insbesondere werden aus der Leitlinie der Arbeitsgruppe Künstliche Intelligenz (Bund) folgende wichtige Erkenntnisse gewonnen:

Der Schweizerische Bund will im Zusammenhang mit dem Einsatz und der Entwicklung von Systemen der künstlichen Intelligenz

- Transparenz, Nachvollziehbarkeit und Erklärbarkeit der Systeme
- zweckgebundene Erhebung und Verwendung von Daten nach ethischen Standards sowie auch die Sicherung der Interoperabilität der Datensysteme
- hohe Rechtssicherheit und Innovation durch den Einsatz von KI-Systemen

erreichen bzw. gewährleisten. Zu diesen Zielen bzw. Absichten können Standards einen grossen Beitrag leisten. In den Standards können Konzept, Regeln, Methoden u.ä. definiert und mit den Akteuren der Öffentlichkeit inhaltlich abgestimmt werden. Sowohl aus den Beiträgen als auch in den Studien dieser Arbeit kann man entnehmen, dass der Einsatz von KI-Standards Vertrauen und Rechtssicherheit für die Anwendung von Systemen im Bereich künstliche Intelligenz schaffen.

Auch dem Verordnungsentwurf der EU kann entnommen werden, dass das Potenzial für KI-Standards erkannt wurde. Im Grundsatz geht es aber auch darum, Vertrauen und Akzeptanz zu schaffen. Mit dem Einsatz von KI-Standards könnten die Grundsätze und Anforderungen aus dem Verordnungsentwurf für die Praxis gut übersetzt und vollzogen werden.

Im öffentlichen Bereich bzw. im Kontext von eGovernment können KI-Standards wichtige Sicherheitsaspekte abdecken sowie auch finanzielle Vorteile anbieten. Einheitliche KI-Standards können bei der Entwicklung und beim Einsatz von smarten Assistenten im Bereich eGovernment nicht nur Kriterien aus nationalen und internationalen Regulierungen erfüllen, sondern auch einen schnellen Fortschritt in der Innovation des eGovernments fördern. Insbesondere werden mit Standards im öffentlichen Bereich folgende Anforderungen erfüllt:

- Kompatibilität, Interoperabilität, Sicherheit und Qualität
- Einheitlichkeit der Anwendung sowie Einbezug der Stakeholder
- Zukunftsfähigkeit, Wirtschaftlichkeit und Nachhaltigkeit
- Nachvollziehbarkeit und Transparenz
- Flexibilität und Innovationsfähigkeit
- Rechtssicherheit bei der Formulierung von Verträgen und Ausschreibungen

# 8 Empfehlungen

Der Einsatz der künstlichen Intelligenz wird sich in den nächsten Jahren auch in der öffentlichen Verwaltung etablieren. Standards können den Entwicklern und Anwendern der KI helfen, wichtige normative Vorgaben aus den Gesetzen, Verordnungen gut zu übersetzen und bei der Umsetzung unterstützen. Aus den Beiträgen der Bundesverwaltung bzw. ihrer Departemente sieht man, dass ein grosser Bedarf an Standards besteht. eCH könnte in dieser Angelegenheit einen Beitrag leisten.

Anhand der Erkenntnisse aus der vorliegenden Analyse wird dem eCH folgende Empfehlungen vorgeschlagen:

- Aufnahme des Themas "Standards für künstliche Intelligenz" in die Agenda der künftigen Aktivitäten von eCH und Steuerung dieses Themas durch den Vorstand oder Expertenausschuss
- Monitoring der Aktivitäten der Bundesverwaltung im Zusammenhang mit den KI-Standards oder und KI-Regulierung sowie ein Informationsaustausch bei Bedarf, insbesondere mit den Bundesämter BAKOM und EDA als Treiber des Themas beim Bund
- Bildung einer neuen Fachgruppe für die Erarbeitung von technischen Standards für künstliche Intelligenz, bestehend aus den Vertretern vom BAKOM, EDA und Experten aus der Wirtschaft sowie auch Zusammenarbeit mit europäischen Organisationen, die KI-Standards entwickeln
- Zusammenarbeit mit dem Kompetenznetzwerk für künstliche Intelligenz (CNAI: Competence Network for Artificial Intelligence / Kompetenznetzwerk für KI). Dieser Punkt ist im Interview mit dem Kompetenznetzwerk für künstliche Intelligenz thematisiert worden. Das Kompetenznetzwerk KI könnte ein Knoten «technische KI-Standards» schaffen, in welchem eCH den Lead für KI-Standardisierungen im Bereich E-Government in der Schweiz übernimmt.

# 9 Literaturverzeichnis

Buxmann, P., & Schmidt, H. (2019). *Künstliche Intelligenz - Mit Algorithmen zum wirtschaftlichen Erfolg.* Springer-Verlag.

eGovernment Schweiz. (n.d.). Was ist E-Government? https://www.egovernment.ch/index.php/download_file/491/3344/

Europäische Kommission. (2021). Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206

Kreutzer, R., & Sirrenberg, M. (2019). *Künstliche Intelligenz verstehen.* Springer Verlag.

Staatssekretariat für Bildung, Forschung und Innovation SBFI. (2020). *Leitlinien "Künstliche Intelligenz" für den Bund.* https://www.sbfi.admin.ch/sbfi/de/home/bfi-politik/bfi-2021-2024/transversale-themen/digitalisierung-bfi/kuenstliche-intelligenz.html

The Open Community for Ethics in Autonomous and Intelligent Systems (OCEANIS). (n.d). *Repository*. https://ethicsstandards.org/repository/

VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V. (2020). *Alles rund um den Normungsprozess.* https://www.dke.de/de/normen-standards/grundlagen-der-normung/normungsprozess

Wahlster, W. & Winterhalter, C. (2020). *Deutsche Normungsroadmap Künstliche Intelligenz*. DIN.

Wikipedia. (n.d.). *Standard*. https://de.wikipedia.org/wiki/Standard