Fridel Rickenbacher ist ehemaliger Mitgründer, Co-CEO, Partner, Verwaltungsrat und nun beteiligter «Unternehmer im Unternehmen» / «Senior Consultant» bei der Swiss IT Security AG / Swiss IT Security Group. Auf Bundesebene ist er als Experte und Akteur vertreten bei «Digital Dialog Schweiz» + «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS». Er ist in seiner Mission «sh@re to evolve» seit Jahren als Redaktionsmitglied, Experten-Gruppen-

AI Readiness Strategie – «Un-Hype the Hype» mit Fokus auf «Stand der Technik»

Der Hype rund um die künstliche Intelligenz (KI/AI) und der sogenannten, inflationär referenzierten «AI Readiness / AI Strategie» zeigen bei vielen Organisationen auch nicht gemachte Hausaufgaben auf. Wie schon länger die «Digital Transformation» ist auch die «künstliche Intelligenz (KI/AI)» bzw. die entsprechende «AI Readiness» letztlich eine forcierte, immer dynamisch werdende Komponente / Weiterentwicklung gemäss «Stand der Technik». Nebst der technischen Dynamik bezüglich «Stand der Technik» ist die organisatorische Dynamik in Zukunft kaum mehr zu schaffen, wenn eine Zukunfts-Kompetenz wie z.B. die «Wandlungsfähigkeit» fehlt im «Mindset» der betroffenen Akteure.

«AI Readiness» – weiteres Kern-Element der «agilen Planung in der ICT Digital-DNA-Strategie»

Eine AI Readiness Strategie ist eine wichtige Planungsgrundlage, welche mitunter beschreibt, wie eine Organisation die KI in ihre bestehenden und zukünftigen Geschäftsmodelle adaptieren und integrieren kann. Dabei geht es nicht nur um die Auswahl und Implementierung von KI-Tools, sondern auch um die Anpassung der organisatorischen Strukturen, Prozesse und Kulturen an die neuen Anforderungen und Möglichkeiten, die die KI mit sich bringt. In Wissen und Relation, dass die KI «nur» ein unterstützendes, aber sehr, sehr mächtiges Tool ist, in einem «intelligent orchestrierten» Gesamtsystem braucht es hier eine sehr differenzierte Betrachtung und organisationsfokussierte Evaluation. Eine «AI Readiness» sollte ein integriertes Kern-Element der «agilen Planung in der ICT-Strategie / Digital-DNA-Transformation» darstellen und folgende Beispiel-Elemente / Aspekte berücksichtigen:

Wert-Realisierungs- und Adoption-Planung

Eine solche definiert mitunter, wie das Unternehmen den Nutzen der künstlichen Intelligenz / Digital-DNA-Transformation in Schritten realisieren, messen und maximieren will, welche lohnenswerten Initiativen priorisiert und eingeführt werden sollen, welche Chancen und Innovationen effektiv in die Infrastruktur / Kultur adaptiert werden, welche Ressourcen benötigt werden, und wie der Erfolg (z. B. in Effizienzsteigerung, Qualität, Produktoptimierungen, Kundenzufriedenheit, neue Kompetenzen usw.), aber auch die Akzeptanz oder das Vertrauen der betroffenen Akteure bewertet werden.

Erweiterte Entscheidungsgrundlagen

Um die KI zu verstehen und zu nutzen, sollte eine Organisation zuerst die mitunter seit Jahrzehnten angewachsene, teilweise unstrukturierte Datenqualität und -verfügbarkeit bereinigen, reorganisieren und erhöhen, die Datenanalyse und -interpretation verbessern und die Datenkommunikation und -visualisierung vereinfachen. Dabei sollte sie auch die KI als einen Partner / Support-Technologie betrachten, welche die menschliche Intuition und Kreativität ergänzen und erweitern kann nach einer solchen initialen «know your data»-Phase (Kenne deine Daten) für danach realisierbare, optimierte und letztlich darauf basierende präzisere Entscheidungsgrundlagen in der Zukunft.

Business Intelligence and Excellence

Um die KI zu bewerten und zu verbessern, sollte eine Organisation die Leistung und den Wert der KI bzw. deren Impacts auf die Organisation messen und überwachen, relevante und hilfreiche Feedback- und Lernschleifen etablieren und die kontinuierliche Verbesserung fördern. Dabei sollte sie auch die KI als einen mithelfenden Treiber für Innovation und Exzellenz betrachten, welche gar auch neue Geschäftschancen und

und Verbands-Aktivist tätig bei z. B. SwissICT, s-i.ch, isss.ch, isaca.ch, bauen-digital.ch rund um Digitalisierung, Engineering, Clouds, ICT-Architektur, Security, Privacy, Datenschutz, Audit, Compliance, Controlling, Information Ethics, in entsprechenden Gesetzes-Vernehmlassungen und auch in Aus- und Weiterbildung (CAS, eidg. dipl.).

weitergehende Wettbewerbsvorteile schaffen kann. Aber auch hier ist entscheidend, dass es für diesen Aspekt «keine gute künstliche Intelligenz / Algorithmen / Tools geben kann ohne die menschliche Intelligenz als Grundlage».

Prototyping
Um die Potenziale und Grenzen der KI zu erkunden, sollte eine Organisation experimentierfreudig sein und verschiedene KI-Lösungen / Tools / Apps testen, evaluieren und iterieren. Dies natürlich immer auch in Abhängigkeit der möglichen Rahmenbedingungen je nach Branche und geltenden Regulationen. Dabei sollte sie sich nicht nur auf die technische Machbarkeit, sondern auch auf die ethische Vertretbarkeit, die rechtliche Konformität und die wirtschaftliche Rentabilität der KI-Projekte konzentrieren. Dies auch speziell mit «baby steps» in der Erarbeitung / Prototyping von «Use Cases» (identifizierte Anwendungsfälle, welche z. B. Optimierungen und Effizienzsteigerungen in der Organisation mit sich bringen nach deren Verankerung in den Prozessen). Bei Bedarf bewusst mit auch dem Ansatz von «fail fast» im Sinne von «vielen Anläufen und Versuchen von Tests / Iterationen mit schnellen, aber auch sofort korrigierbaren Erkenntnissen zugunsten von erst genau dadurch realisierbarem Lernprozess».

Effizienz
Um KI effektiv und effizient zu nutzen, sollte eine Organisation ihre bestehenden Geschäftsprozesse analysieren und optimieren, um unnötige Komplexität, Redundanz und Verschwendung zu reduzieren zugunsten des Effizienz-Zieles. Dabei sollte sie auch die KI als einen Faktor berücksichtigen, der die Prozesse beschleunigen, vereinfachen und verbessern kann im entsprechenden daraus sich hoffentlich auch weiter entwickelbaren «Toolset» / «Skillset» und «Mindset» der Organisation.

Automation
Um die KI zu skalieren und zu standardisieren, sollte eine Organisation die Automatisierung von Routineaufgaben und Entscheidungen anstreben, die von der KI besser und schneller erledigt werden können als von Menschen. Dabei sollte sie aber auch die menschliche Kontrolle und Überwachung der KI sicherstellen, z. B. auch mit «Critical Thinking», um Fehler, Missbrauch und letztlich gar einen Vertrauensverlust in solche neuesten Technologien zu vermeiden.

«Rules before Tools» – Regeln bevor neue Werkzeuge zum Einsatz kommen
Bevor eine Organisation die KI implementiert und anwendet, sollte sie jedoch einige grundlegende Regeln und auch ICT Security Policy / Compliance Definitionen beachten, die den Datenschutz / Datensicherheit, die Qualität und die Nachhaltigkeit bis hin zur Ethik der KI und Digital-DNA-Transformation gewährleisten. Folgende Beispiele einer solchen Regel / Grundlage können hier helfen:

ICT Security Policy
Eine Organisation sollte eine klare und konsistente Richtlinie für die Informationssicherheit (Datenschutz und Datensicherheit) haben, die die Ziele, die Verantwortlichkeiten, die Regeln, Weisungen, Massnahmen und die Kontrollen für den Schutz der Daten, Berechtigungen und der Systeme vor internen und externen Bedrohungen definiert. Dabei sollte sie auch die spezifischen Risiken und Herausforderungen berücksichtigen, die die KI mit sich bringt, wie z. B. die Anfälligkeit für Manipulation, die Abhängigkeit von Drittanbietern, Urheberrechtsfragen, Schutz von personenbezogenen oder firmenkritischen Informationen und bis hin zur gar einer Unvorhersehbarkeit des Verhaltens oder Outputs mit Folgeauswirkungen.

Sensibilisierung und Aufklärung
Eine Organisation sollte das Bewusstsein und das Verständnis für die KI bei allen Stakeholdern / Akteuren fördern, die von der KI betroffen sind oder die KI bzw. deren Anwendung auch mitgestalten können. Dabei sollte sie nicht nur die Vorteile und die Chancen, sondern auch die Grenzen und die Risiken der KI transparent und ehrlich kommunizieren, um falsche Erwartungen, Ängste und Widerstände zu vermeiden. Erst mit einem richtigen, an die Organisation angepasstem «Mindset» (Einstellung, Richtung der Gedanken) und ausgewogenen Rahmenbedingungen kann erst die passende KI-Anwendung und Innovation zielführend Einzug halten.

Critical Thinking / gesunder Menschenverstand
Eine Organisation sollte das kritische Denken «Critical Thinking» und die Urteilsfähigkeit bei allen Stakehol-

Fortsetzung Seite 14

dern / Akteuren stärken, die mit der KI interagieren oder letztlich abschliessend entscheiden müssen. Dabei sollte sie nicht nur die technischen und funktionalen Aspekte, sondern auch die ethischen und sozialen Auswirkungen der KI berücksichtigen, um verantwortungsvolle und nachhaltige Entscheidungen zu treffen bei der Anwendung / Weiternutzung / Weitergabe von KI-Outputs.
Die mitunter gefährliche Systemgläubigkeit bei vor allem AI-Fehlinformationen aber auch bei Social Engineering / Cybercrime Attacken ist mittels neuer Kompetenzen wie z. B. «Critical Thinking» oder auch durch den guten alten «gesunden Menschenverstand» zu reduzieren -> Ein Prinzip findet hier auch Anwendung «Zero trust, always verify». Der gesunde Menschenverstand / «Common sense» ist auch kulturell und gesellschaftlich unterschiedlich geprägt über Generationen und entsprechend sehr komplex. Dieses Selbstverständnis bezüglich dieses Verstandes für uns Menschen ist auch für die «stärkste» KI sehr schwer oder (noch) gar nicht zu verstehen.

Schulungen und neue Kompetenzen
Eine Organisation sollte die Kompetenzen und Fähigkeiten bei allen Stakeholdern / Akteuren entwickeln, die die KI nutzen oder die KI gestalten müssen. Dabei sollte sie nicht nur die fachlichen und methodischen Kenntnisse, sondern auch die persönlichen und sozialen Fertigkeiten («Toolset», «Skillset») vermitteln, um die KI effektiv und effizient zu bedienen, zu überwachen, zu verbessern und zu innovieren. Menschen werden nicht einfach so durch die KI ersetzt, jedoch werden Menschen gar mal «ersetzt» mit Menschen, welche mit KI umgehen und interagieren können. Wie früher erwähnt: Nebst der technischen Dynamik bezüglich «Stand der Technik» ist die organisatorische Dynamik in Zukunft kaum mehr zu schaffen, wenn eine Zukunfts-Kompetenz wie z. B. die «Wandlungsfähigkeit» fehlt im «Mindset» der betroffenen Akteure.

NoCode / LowCode
Eine Organisation sollte die Zugänglichkeit, Qualität und die Benutzerfreundlichkeit der KI erhöhen und trainieren, indem sie Plattformen, Werkzeuge, Apps, Vorlagen anbietet, die es den Stakeholdern / Akteuren ermöglichen, KI-basierte Tools ohne oder mit wenig Programmierkenntnissen zu erstellen, zu konfigurieren und zu modifizieren. Genau hier braucht es aber mitunter ein sehr vertieftes, «menschliches» Grundverständnis und genaue Analyse-/ Beschreibungskompetenz des zu lösenden Problems oder zur z. B. erreichenden Optimierung / Automatisierung / Effizienzsteigerung.
Dabei sollte die Organisation aber auch die Qualität und die Zuverlässigkeit sicherstellen, indem sie Standards und Richtlinien für die Entwicklung, die Prüfung und die Freigabe solcher KI-Anwendungen auf Basis von «NoCode» / «LowCode» festlegt.

Compliance
Eine Organisation sollte die Rechtmässigkeit und die Konformität der KI gewährleisten, indem sie die geltenden Gesetze, Vorschriften, Organisationsrichtlinien, ICT Security Policy und Normen einhält, die die KI regulieren oder beeinflussen. Dabei sollte sie auch die Anforderungen und Erwartungen der Stakeholder / Akteure erfüllen, die die KI bzw. deren Outputs überwachen oder bewerten, wie z. B. die Behörden, die Kunden, die Partner und die Gesellschaft.

Business Continuity Planning
Eine Organisation sollte die Verfügbarkeit und die Widerstandsfähigkeit (Resilienz) und letztlich die Angriffs- und Betriebssicherheit der KI bzw. den darauf basierten Tools / Apps / Schnittstellen sicherstellen, indem sie Pläne und Massnahmen für den Fall von Störungen, Ausfällen, Katastrophen und auch Datenschutz-/Cybercrime-Vorfälle vorbereitet, die die KI beeinträchtigen oder unterbrechen können. Dabei sollte sie auch die Alternativen und die Notfalllösungen (z. B. Notfall-Betrieb während Inci-

dent Response / Business Recovery, halb-automatische Betrieb usw.) bereitstellen, die die KI ersetzen oder ergänzen können, wenn die KI nicht oder «falsch» funktioniert oder nicht verfügbar ist.

Datenschutz-Folgenabschätzung
Eine Organisation sollte die Privatsphäre und die Persönlichkeitsrechte der Stakeholder / Akteure / Kunden / Mitarbeiter schützen, indem sie die potenziellen Auswirkungen der KI auf die Verarbeitung personenbezogenen oder firmenkritischen Daten analysiert und bewertet. Dabei sollte sie auch die Massnahmen ergreifen, die die Risiken und die Nachteile der KI minimieren oder beseitigen, wie z. B. Security by design, security by default, privacy by design, privacy by default, die Anonymisierung, die Pseudonymisierung, die Verschlüsselung und die Löschung der Daten.

Strategisches Daten- und App-Management – «know your data and apps»
Die KI ist stark abhängig bzw. aufbauend von den Daten und den Anwendungen, die sie speist, die sie nutzt und trainiert. Daher ist es für eine Organisation unerlässlich, ein strategisches Daten- und App-Management aufzubauen und weiterzuentwickeln, welches die Qualität, die Sicherheit und die Nachhaltigkeit der Daten und der Anwendungen gewährleistet in einer möglichst nachhaltigen Weiterentwicklung und Spezialisierung mit der diesbezüglich unterstützenden KI. Ein strategisches Daten- und App-Management sollte folgende Beispiel-Aspekte umfassen:

Datenschutz
Eine Organisation sollte die Einhaltung der Datenschutzgesetze und -richtlinien sicherstellen, die die Verarbeitung personenbezogenen oder firmenkritischen Daten regeln oder beeinflussen. Dabei sollte sie auch die Rechte und Interessen der Betroffenen respektieren und schützen, wie z. B. das Recht auf Auskunft, Berichtigung, Löschung, Widerspruch, Datenminimierung und Datenübertragbarkeit. Dazu gehören auch Konzepte und Ansätze von z. B. «privacy by design» oder «privacy by default».

Datensicherheit
Eine Organisation sollte die Sicherheit der Daten und der Anwendungen gewährleisten, die die KI speist und nutzt. Dabei sollte sie geeignete technische und organisatorische Massnahmen ergreifen, um die Daten und die Anwendungen vor unbefugtem Zugriff, Verlust, Beschädigung, Manipulation oder Missbrauch bis hin zu auch z. B. Erpressung durch Cybercrime-Organisationen zu schützen. Dazu gehören z. B. «Security by design», «security by default», die Verschlüsselung, die Authentifizierung, die Zugriffskontrolle und die Überwachung.

Auftragsdatenverarbeiter-Verzeichnis
Eine Organisation sollte ein Verzeichnis führen, welches alle Auftragsdatenverarbeiter / Kern-Applikations-Lieferanten und entsprechende relevante Partner auflistet, die im Rahmen der KI-Nutzung personenbezogene oder firmensensitive Daten – auch speziell entwickelte Algorithmen / Codes / Scripts / Apps usw. – im Auftrag der Organisation verarbeiten oder speichern. Dabei sollte sie auch die Art, den Umfang, den Zweck und die Dauer der Datenverarbeitung sowie die Gewährleistungen für die Einhaltung der Datenschutzvorschriften, «Stand der Technik» oder akzeptierte «best practices» / «good practices» dokumentieren.

Know-how-Management
Eine Organisation sollte das Wissen / Dokumentation und die spezialisierten Fähigkeiten über die Daten und die entwickelten Anwendungen, die die KI speist und nutzt, aufbauen und – auch gar extern durch Dritte auditierbar – pflegen. Dabei sollte sie auch die Kompetenzen und die Verantwortlichkeiten für die Daten- und App-Verwaltung klar definieren und verteilen auf «mehrere Know-how-Träger», bei Bedarf und je nach Kritikalität auch unterstützt durch externe Spezialisten. Dazu gehören z. B. auch die erweiterte Daten- und App-Modellierung, -Bereinigung, -Anreicherung, -Analyse, -Visualisierung / Dokumentation und -Aktualisierung bei kritischen Kernapplikationen. Solche speziellen Massnahmen gelten auch erweitert bei speziell schützenswerten Anwendungen und Methoden gegenüber Mitbewerbern (Intellectual Property / geistiges Eigentum).

Evaluationen von neuen Systemen / Tools / ERP
Eine Organisation sollte die Eignung und die Auswirkungen von neuen Systemen, Tools oder ERP, die die KI speisen oder nutzen, sorgfältig prüfen und bewerten. Dabei sollte sie auch die Anforderungen und die Erwartungen aller Stakeholder und vorallem internen Akteuren berücksichtigen und einbeziehen. Dazu gehören z. B. die Integration in KI-/Cloud-Systemen, Kompatibilität, Schnittstellen-Unterstützung, nutzbare API, App-Verfügbarkeit auf diversen Plattformen, Funktionalität, die Benutzerfreundlichkeit, die Kompatibilität, die Skalierbarkeit, die Kosten, die messbare Leistung und Nachhaltigkeit des zukunftsorientierten Nutzens. Diese Evaluation muss in mehreren Aspekten weiter gehen bis hin zur z. B. Unterstützung der maximierten Angriffs- und Betriebssicherheit, Datenschutz, Datensicherheit in der dynamischen Bedrohungslage gemäss «Stand der Technik».

Arbeitgeberattraktivität mittels Digital-DNA-Maturität im Fachkräftemangel
Die KI erfordert nicht nur eine technologische, sondern auch eine kulturelle Transformation in den Organisationen. Daher ist es für eine Organisation schon länger essenziell, eine attraktive visible Arbeitgebermarke zu entwickeln, welche die Digital-DNA-Maturität widerspiegelt und entsprechend gar auch die «am besten passenden» Fachkräfte anzieht, motiviert und bindet, die für die KI-Nutzung erforderlich sind.

Fortsetzung Seite 16

Eine attraktive Arbeitgebermarke bei auch entsprechend zu forcierenden Visibilität im Marktumfeld sollte folgende Beispiel-Aspekte umfassen:

Talent Management
Eine Organisation sollte ein systematisches und strategisches Talent Management fördern, welches die Identifizierung, die Rekrutierung, die Entwicklung, die Förderung und die Bindung der Fachkräfte für die KI-Nutzung und Digital-DNA-Transformation ermöglicht. Freie Getränke, frisches Obst, Homeoffice-Optionen und leistungsgerechte Entlöhnung reichen hier längst nicht mehr bzw. sind auch mittlerweile vorausgesetzter Standard im harten Wettbewerb im Rahmen des Fachkräftemangels.

Innovationskultur
Eine Organisation sollte eine innovationsfreundliche, möglichst auch digitalisierte Kultur («Mindset») haben, welche die Kreativität, die Experimentierfreude («Fail Fast»), die Risikobereitschaft und die Lernfähigkeit der Fachkräfte für die KI-Nutzung unterstützt und auch gar der Mitgestaltung belohnt. Dabei sollte sie auch die Zusammenarbeit, den Austausch und die Vernetzung der Fachkräfte über Abteilungen, Funktionen und Hierarchien hinweg erleichtern und anregen, z. B. auch mit guten alten ERFA (Erfahrungsaustausch Gruppen).

Future Skilling
Eine Organisation sollte eine kontinuierliche und zielgerichtete Weiterbildung und bei Bedarf gezielte Umschulung der Fachkräfte für die KI-Nutzung und Digital-DNA-Transformation anbieten und ermöglichen. Dabei sollte auch der aktuelle und vor allem zukünftige Kompetenzbedarf und -lücken analysiert und adressiert werden. Dazu gehören z. B. die technischen, die methodischen, die persönlichen und die sozialen Kompetenzen. Man kann es nicht genug wiederholen: Nebst der technischen Dynamik bezüglich «Stand der Technik» ist die organisatorische Dynamik in Zukunft kaum mehr zu schaffen, wenn eine Zukunfts-Kompetenz wie z. B. die «Wandlungsfähigkeit» fehlt im «Mindset» der betroffenen Akteure.

Toolset/Skillset/Mindset
Eine Organisation sollte die passenden Werkzeuge «Toolset», Fähigkeiten «Skillset» und Einstellungen «Mindset» für die Digital-DNA-Transformation und KI-Nutzung entwickeln, möglichst allen bereitstellen und proaktiv fördern gemäss auch «Stand der Technik». Dabei sollte sie auch die Anpassungsfähigkeit, die Flexibilität und die Agilität der Fachkräfte für die Digital-DNA-Transformation und KI-Nutzung stärken und fordern. Dazu gehören z. B. die Plattformen, die Apps, die Vorlagen, die Frameworks, die Algorithmen, die Daten, die Modelle, die Schnittstellen, die Prozesse, die Methoden, die Prinzipien, die Werte und die darauf aufgebauten Visionen und realisierbaren Innovationen.

KI als weiteres «Zünglein an der Waage» für digitale Verwaltung bis zu eGovernment?

Die KI und Digital-DNA-Transformation bietet nicht nur für die Privatwirtschaft, sondern auch für die öffentliche Verwaltung viele Möglichkeiten, die Leistung, die Effizienz und die Qualität der Dienstleistungen zu verbessern und die Zufriedenheit, die Partizipation (z. B. Digitale Bürgernähe) und das Vertrauen der Bürgerinnen und Bürger zu erhöhen. Doch wie kann die öffentliche Verwaltung die KI nutzen, ohne die Komplexität, die Sicherheit, die Compliance und die Transparenz zu beeinträchtigen? In diesem Abschnitt werden einige Herausforderungen und Lösungsansätze für das eGovernment mit KI und Digital-DNA-Transformation erörtert:

Komplexität des Applikationsportfolios
Die öffentliche Verwaltung verfügt oft über ein sehr umfangreiches und heterogenes Applikationsportfolio, das aus verschiedenen Systemen, Plattformen, Schnittstellen und Datenbanken besteht, die teilweise veraltet, inkompatibel oder redundant sind. Dies erschwert die Integration, die Aktualisierung und die Erweiterung der Applikationen mit KI und Cloud Services. Eine mögliche (aber sehr theoretische …) Lösung ist die Vereinheitlichung, die Vereinfachung / strategische Konsolidierung und die Standardisierung des Applikationsportfolios, z. B. durch die Nutzung von Cloud-Diensten, die Modularisierung von Systemen, die Harmonisierung von Schnittstellen und die Konsolidierung von Datenbanken. Aufgrund auch z. B. der Komplexität und auch je nach Grösse dauern solche Projekte mehrere Jahre im Vergleich zu kleineren, teilweise agileren Organisationen und KMU.

Legacy Applikationen und entsprechende Prozesse
Die öffentliche Verwaltung nutzt oft Legacy Applikationen, die auf veralteten Technologien, Architekturen oder Paradigmen basieren, die nicht für die KI geeignet oder anpassbar sind. Dies verhindert die Nutzung, die Anpassung und die Verbesserung der Applikationen mit KI. Eine mögliche Lösung ist die schrittweise Modernisierung, die (Teil)Migration oder die Ablösung der Legacy Applikationen, z. B. durch die Nutzung von No-Code/Low-Code-Plattformen, Middleware, Schnittstellen, die Umstellung auf Microservices, die Einführung von KI-Modulen oder die dann aber sehr zeit- und kostenintensive Entwicklung von neuen Applikationen.

Datenschutz- und Compliance-Vorgaben
Die öffentliche Verwaltung unterliegt oft strengen Datenschutz- und Compliance-Vorgaben, die die Verarbeitung personenbezogener Daten oder sensibler Informationen regeln oder einschränken. Dabei muss sie auch die Rechte und Pflichten der Bürgerinnen und Bürger sowie der Aufsichtsbehörden beachten und erfül-

len. Eine mögliche Lösung bzw. Grundlage für weitere Schritte ist die Anwendung von Datenschutz-Folgenabschätzungen, die die potenziellen Auswirkungen der KI auf die Privatsphäre und die Persönlichkeitsrechte analysieren und bewerten, sowie die Implementierung von security by design, security by default, privacy by design, privacy by default, die die datenschutzfreundlichsten Einstellungen und Massnahmen vorsehen und umsetzen.

Langjährige Software- und Partner-Verträge

Die öffentliche Verwaltung ist oft an langjährige Software- und Partner-Verträge gebunden, die die Nutzung, die Anpassung und die Erneuerung der Applikationen mit KI und Cloud Services einschränken, verzögern oder verhindern. Dabei muss sie auch die Kosten, die Nutzungsbedingungen und die Haftungsfragen berücksichtigen und klären. Ein langwieriger Prozess und steiniger Weg (teilweise dann mit Neuevaluationen und Ausschreibungen verbunden) ist die Verhandlung, die Anpassung oder die Kündigung der Software- und Partner-Verträge, die Flexibilisierung von Lizenzmodellen, die Vereinbarung von weitergehenden Service-Level-Agreements in der Übergangsphase (teilweise mit auch anderen unterstützenden Partnern) oder die Ausübung von Exit-Klauseln.

Statische ICT-Strategie versus agile ICT-Planungsstrategie

Die öffentliche Verwaltung verfolgt oft eine historisch gewachsene, gegebene, statische ICT-Strategie, die die Ziele, die Massnahmen und die Ressourcen für die Nutzung, die Anpassung und die Erneuerung der Applikationen mit KI und Cloud Services nicht uneingeschränkt / nicht zu agil definieren oder aktualisieren kann. Dabei muss sie auch die Dynamik, die Unsicherheit und die Komplexität des technologischen Wandels berücksichtigen und antizipieren. Eine möglicher, aber natürlich sehr theoretischer Ansatz ist die Entwicklung, die Implementierung und die Überprüfung einer agilen ICT-Strategie zugunsten der Antizipierung der herrschenden Dynamik im technologischen Universum, z. B. durch die Nutzung von Szenario-Planung, die Etablierung von Prototyping / Feedback-Schleifen, die Förderung von Experimentier-Räumen (Fail fast, NoCode / LowCode) oder die Anwendung von gar auch agilen und Lean-Start-up-Methoden.

«Ohne oder mit KI» das neue Gütesiegel?

Die Frage, ob eine Organisation ohne oder mit KI arbeitet, wird immer relevanter und entscheidender für ihren Erfolg und ihr Image im hart umkämpften Wettbewerb und speziell auch dem Fachkräftemangel. Dabei geht es nicht nur um die technologische Kompetenz, sondern auch um die strategische Ausrichtung, die kunden- und mitarbeiterorientierte Differenzierung und die gesellschaftliche Verantwortung. Eine Organisation, die mit KI und Digital-DNA-Transformation arbeitet, sollte daher folgende Beispiel-Aspekte beachten:

Mehrwerte / Use cases messbar machen

Eine Organisation sollte die konkreten Ziele und Nutzen definieren, die sie mit der KI und Digital-DNA-Transformation erreichen will und diese anhand von messbaren Indikatoren / Adoption Scoring überprüfen und bewerten. Dabei sollte sie auch die Kosten, die Risiken und die Nebenwirkungen der KI berücksichtigen und minimieren. Dazu gehören z. B. die Verbesserung der Qualität, der Effizienz, der Kundenzufriedenheit, der Innovation, der Wettbewerbsfähigkeit, der Arbeitgeberattraktivität und der Nachhaltigkeit.

Digitale Kunden- und Bürgernähe

Eine Organisation sollte die Bedürfnisse, die Erwartungen und die Präferenzen der Kunden und der Bürger verstehen, antizipieren und erfüllen, indem sie die KI und Digital-DNA-Transformation nutzt, um personalisierte, relevante und wertvolle Dienstleistungen und Produkte anzubieten (wie z. B. 7 × 24 h digitaler Schalter, Self Services, Mehrwert Portal). Dabei sollte sie auch die Transparenz, die Fairness und die Sicherheit der KI und Digital-DNA-Transformation gewährleisten und die Einwilligung, die Mitgestaltung, die Kontrolle und das Feedback der Kunden und der Bürger ermöglichen und respektieren.

Fortsetzung Seite 19

AI Regulationen gegen die Angst oder zugunsten der Hoffnung

Die KI wirft nicht nur technische, sondern auch ethische, rechtliche und soziale Fragen und Herausforderungen auf, die eine angemessene Regulierung erfordern, um die Sicherheit, die Qualität und die Akzeptanz der KI zu sichern und zu fördern. Dabei geht es nicht nur um die Beschränkung, sondern auch um die Ermöglichung, die Förderung und die Orientierung der KI. Eine Organisation, die mit KI arbeitet, sollte daher folgende Beispiel-Aspekte beachten:

Datenschutz-Regulationen

Eine Organisation sollte die Einhaltung der Datenschutz-Regulationen sicherstellen, die die Verarbeitung personenbezogener oder firmenkritischer Daten durch die KI regeln oder beeinflussen. Dabei sollte sie auch die Rechte und Interessen der Betroffenen respektieren und schützen, wie z. B. das Recht auf Auskunft, Berichtigung, Löschung, Widerspruch und Datenübertragbarkeit. Dazu gehören z. B. die Datenschutz-Grundverordnung (DSGVO) der EU, die seit 2018 gilt, die Datenschutz-Prinzipien-Regelung (DPGR) der Schweiz, die seit 2018 gilt, und das neue Datenschutzgesetz (DSG) der Schweiz, das seit dem 1. September 2023 in Kraft ist.

Weitere neueste «AI ACT» Regulationsvorstösse der EU

Eine Organisation sollte die neuesten «AI ACT»-Regulationsvorstösse der EU beachten, die die Entwicklung, den Einsatz und die Überwachung der KI regeln oder beeinflussen. Dabei sollte sie auch die Anforderungen und Erwartungen der Behörden, der Kunden, der Partner und der Gesellschaft erfüllen und einbeziehen. Die EU hat im April 2023 einen Vorschlag für eine Verordnung über künstliche Intelligenz vorgelegt, der einen risikobasierten Ansatz verfolgt, der die KI in vier Kategorien einteilt: verbotene, hochriskante, geringriskante und minimale KI und der entsprechenden Pflichten und Sanktionen festlegt. Der Vorschlag zielt darauf ab, eine Balance zwischen Innovation und Sicherheit zu finden, indem er die Entwicklung und den Einsatz von KI fördert, die dem Wohl der Menschen und der Gesellschaft dient, und gleichzeitig die Grundrechte, die Werte und die Regeln der EU achtet und schützt. Der Vorschlag muss noch vom Europäischen Parlament und dem Rat angenommen werden, bevor er in Kraft treten kann.

Noch keine weitergehende Schweizer AI Regulationen

Die Schweiz hat bisher kein spezifisches Gesetz zur Regelung von KI, sondern wendet die bestehenden Gesetze und Vorschriften an, die für die KI relevant sind, wie z. B. das Datenschutzgesetz, das Urheberrechtsgesetz, das Strafgesetzbuch oder das Haftpflichtgesetz. Die Schweiz beobachtet jedoch die Entwicklungen auf internationaler Ebene, insbesondere in der EU, und prüft, ob Anpassungen oder Ergänzungen des Schweizer Rechtsrahmens erforderlich sind. Die Schweiz beteiligt sich auch aktiv an der Gestaltung von internationalen Standards und Normen für KI, z. B. im Rahmen der OECD, der UNO oder des Europarats.

Swiss AI Initiative ETH Zürich mit Supercomputer in der Schweiz / Tessin

Die ETH Zürich hat im Dezember 2023 die Swiss AI Initiative lanciert, die das Ziel hat, die Schweiz als weltweit führenden Standort für die Entwicklung und Nutzung einer transparenten und vertrauenswürdigen KI zu positionieren. Die Initiative bündelt das Fachwissen von rund einem Dutzend Schweizer Universitäten, Fachhochschulen und Forschungseinrichtungen und will neue Large-Language-Modelle (LLMs) entwickeln und trainieren, die auf Transparenz und Open Source basieren. Die Initiative will auch grundlegende Fragestellungen bei der Entwicklung und Nutzung von LLMs klären, wie z. B. die ethischen, rechtlichen und sozialen Auswirkungen der KI. Zudem will die Initiative die Wissenschaft, die Industrie und die Politik zusammenbringen, um gemeinsam die Entwicklung und den Einsatz der KI in der Schweiz mitzugestalten und voranzutreiben.

Eine zentrale, technische Rolle in der Swiss AI Initiative spielt ein neuer Supercomputer, der im Tessin im Swiss National Supercomputing Centre (CSCS) der ETH Zürich installiert werden soll. Der Supercomputer soll eine Rechenleistung von mehr als 100 Petaflops haben und zu den schnellsten und energieeffizientesten der Welt gehören. Der Supercomputer soll allen Schweizer Hochschulen und Forschungsanstalten zur Verfügung stehen und die Entwicklung und das Training von LLMs ermöglichen und beschleunigen. Der Supercomputer soll auch die Zusammenarbeit und den Austausch zwischen den verschiedenen Akteuren im Bereich der KI fördern und die Schweizer Neutralität und Unabhängigkeit in der KI-Forschung stärken.

Diese Initiative hat entsprechend letztlich auch den Zweck, eine möglichst gute Alternative und Unabhängigkeit gegenüber marktmitbestimmenden Monopolisten wie z. B. Microsoft, Amazon, Google, Meta (wenigstens theoretisch) zu wahren oder zu erlangen.