SWISS INFOSEC

MEET SWISS INFOSEC!

KI-Lifecycle-Management Management und Datenschutz

Swiss Infosec AG: Michael Widmer & Dimitri Korostylev

SWISS INFOSEC

Vorwort zur KI: Der AI Act ist beschlossen

Am 21.5.2024 wurde der AI Act endgültig von der EU-Kommission beschlossen und wird voraussichtlich noch diesen Monat in Kraft treten.

SWISS INFOSEC

AI-Lifecycle

Planung

Identifizierung von Zielen, Anforderungen und Rahmen-bedingungen für das KI-System.

Entwurf

Konzeption der Architektur, Algorithmen und Datenstrukturen des KI-Systems.

Entwicklung

Implementierung und Erprobung des KI-Systems gemäss den Entwürfen.

Umsetzung

Einsatz und Betrieb des KI-Systems in der Praxis.

SWISS INFOSEC

AI-Lifecycle: Planungsphase

In der Planungsphase werden die Ziele, Anforderungen und Rahmenbedingungen für das KI-System identifiziert und definiert.

SWISS INFOSEC

Schlüsselelemente der Planungsphase

Geschäftsziele und Anforderungen

Identifizieren Sie die Geschäftsziele und -anforderungen, die das KI-System erfüllen soll.

Definition des Geschäftsproblems

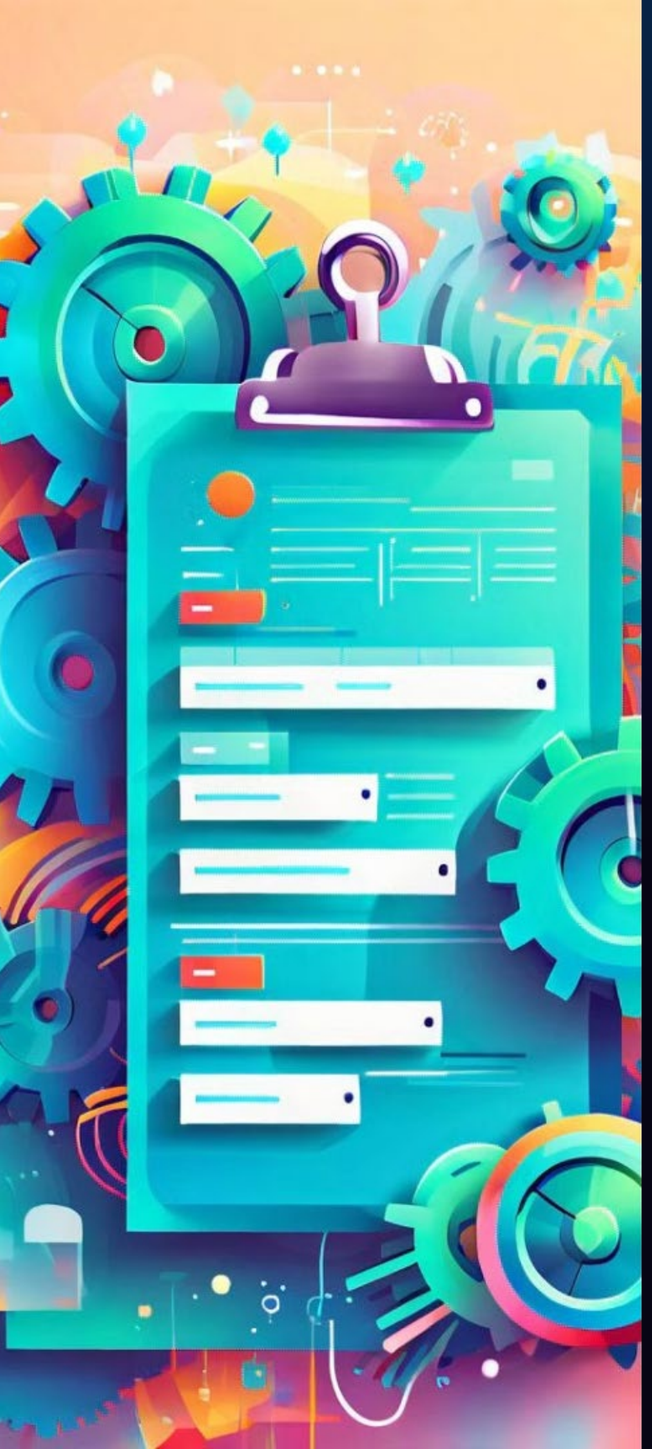
Definieren Sie klar, welche Arten von Problemen das KI-System lösen soll, z.B. Klassifizierung, Regression oder Empfehlungen.

Datenanalyse

Stellen Sie sicher, dass die richtigen Daten für das KI-System verfügbar sind und analysieren Sie diese.

Umfang und Auswirkungen

Legen Sie den Umfang des KI-Systems fest und bewerten Sie dessen Auswirkungen auf das Geschäftsproblem.



Zusammenfassung der Planungsphase

Geschäftsziele und -anforderungen

KI-Experten müssen die Geschäftsziele und -anforderungen berücksichtigen, um das KI-System entsprechend auszurichten.

Definition des Geschäftsproblems

Das Geschäftsproblem, das das KI-System lösen soll, muss klar definiert werden, z.B. Klassifizierung, Regression oder Empfehlungen.

Projektumfang und -governance

Der Projektumfang und die KI-Governance-Struktur mit Verantwortlichkeiten müssen festgelegt werden.

SWISS INFOSEC

AI-Lifecycle: Entwurfsphase

In der Entwurfsphase wird die Architektur, die Algorithmen und die Datenstrukturen des KI-Systems konzipiert.

SWISS INFOSEC

Wichtigste Schritte in der Entwurfsphase

Datenstrategie

Implementierung einer Datenstrategie, die Datenerfassung, -aufbereitung, -bereinigung und -kennzeichnung umfasst.

Systemarchitektur

Festlegung der KI-Systemarchitektur und Auswahl geeigneter Algorithmen.

Datenschutz

Anwendung von PETs wie Anonymisierung, Minimierung und differenzierter Datenschutz

Modellauswahl

Auswahl des KI-Modells entsprechend dem gewünschten Grad an Genauigkeit und Interpretierbarkeit.

SWISS INFOSEC

Vorbereitung in der Entwurfsphase

Daten bereinigen

Fehlerhafte oder irrelevante Daten werden aus dem Datensatz entfernt, um die Qualität und Relevanz der Daten für das KI-System zu verbessern.

Daten kennzeichnen

Die Daten werden mit Tags oder Kommentaren versehen, um ihre Bedeutung und Verwendung für das KI-Modell zu verdeutlichen.

Anonymisierung

Identifikatoren werden aus den Daten entfernt, um die Privatsphäre der Nutzer zu schützen.

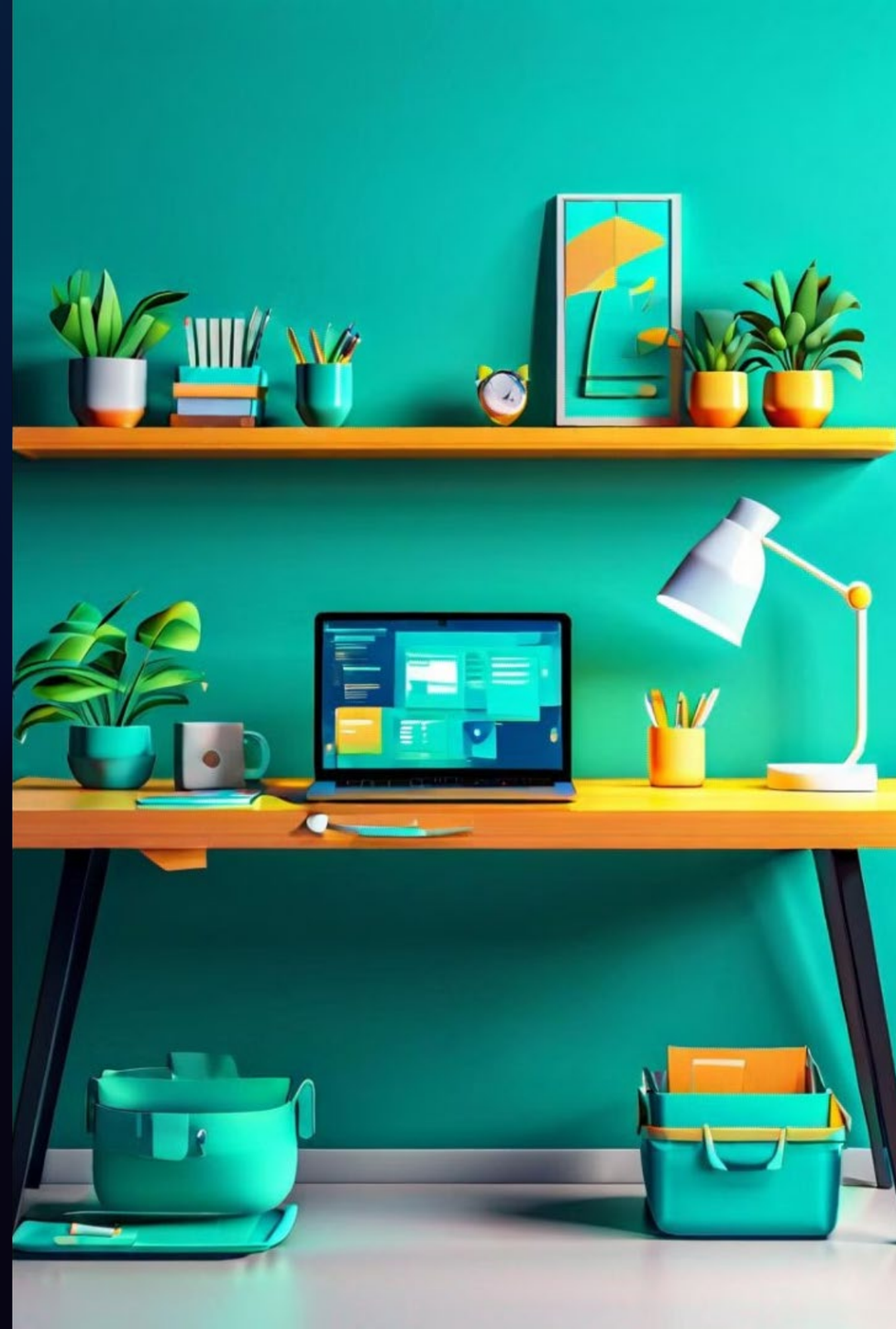
Minimierung

Nur die für das KI-System relevanten Daten werden verwendet, um Datenschutz und -effizienz zu gewährleisten.

SWISS INFOSEC

AI-Lifecycle: Entwicklungsphase

In der Entwicklungsphase wird das KI-System gemäss den Entwürfen implementiert und erprobt.



SWISS INFOSEC

Entwicklungsphase eines KI-Systems

Die wichtigsten Schritte in der Entwicklungsphase eines KI-Systems umfassen das Erstellen des Modells, das Feature Engineering, das Trainieren und Testen des Modells sowie die Verbesserung der Modellleistung.

SWISS INFOSEC

Entwicklungsphase: Kostensenkung & Erklärbarkeit

Kostensenkung

Ziel ist es, die Rechen- und Speicherkosten für Modelle zu senken und die Latenzzeit für Training und Vorhersagen zu verbessern.

Erklärbarkeit

Die Erklärbarkeit/Interpretierbarkeit eines Modells ist wichtig, um Fairness, Datenschutz, Zuverlässigkeit, Robustheit, Kausalität und Vertrauen zu gewährleisten.

Feature Engineering

Durch Verringerung der Merkmale wird die zu verarbeitende und zu speichernde Datenmenge reduziert, was die Effizienz steigert.

SWISS INFOSEC

AI-Lifecycle: Umsetzungsphase

In der Umsetzungsphase wird das entwickelte KI-System in die Praxis überführt. Dabei müssen verschiedene Schritte und Einsatzumgebungen berücksichtigt werden, um das Modell erfolgreich zu implementieren.

SWISS INFOSEC

AI-Lifecycle: Umsetzungsphase

Vor dem Einsatz

Kontinuierliche Überwachung des KI-Modells erforderlich, um Abweichungen zu vermeiden.

Ausgangsbasis festlegen

Festlegung einer Ausgangsbasis zur Messung künftiger Iterationen und Verbesserungen.

Modellpflege

Durchführung von Bereitschaftsanalysen, Einsatz in der Produktion, Überwachung und Validierung des Modells.

SWISS INFOSEC

Einsatzumgebungen

Cloud-basiert

Ein externer Cloud-Anbieter hostet das Modell und kümmert sich um die Infrastruktur. Einfache Skalierung, geringere Investitionen in Hardware, aber mögliche Latenzprobleme und Sicherheitsrisiken.

On-premise

Das Modell wird auf Servern und Hardware gehostet, die sich im Besitz des Unternehmens befinden. Mehr Kontrolle über die Infrastruktur, wichtig für sensible Daten oder regulierte Sektoren, aber höhere Vorabinvestitionen.

Edge

Das Modell wird auf "Edge"-Geräten wie Smartphones gehostet. Geringere Latenzzeiten und mehr Datenschutz, aber mögliche Einschränkungen durch die Hardware-Leistung.

SWISS INFOSEC

Datenschutz

Der Datenschutz ist ein wichtiges Thema bei der Entwicklung und Implementierung von KI-Systemen. Es müssen verschiedene rechtliche Aspekte berücksichtigt werden, um den Schutz personenbezogener Daten zu gewährleisten.

SWISS INFOSEC

Datenschutz & AI: Stand Regulierung Schweiz

Geltendes DSG

Das geltende Datenschutzgesetz ist laut dem EDÖB direkt auf KI-gestützte Bearbeitung von Personendaten anwendbar - ab der Planung und Entwicklung.

Regulierungsansätze

Der Bundesrat evaluiert bis Ende 2024 Ansätze für eine KI-Regulierung, um Transparenz über Zweck, Funktionsweise und Datenquellen zu schaffen.

Governance-Pflichten Pflichten

Bei hohen Risiken besteht eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung, um Datenschutz und Rechte der Betroffenen zu gewährleisten.

SWISS INFOSEC

Datenschutz & AI: Stand Regulierung

AI Act (EU)

Ergänzt die DSGVO und richtet sich an Hersteller, Importeure und Betreiber von KI-Systemen.

Risikobasierter Ansatz

Unannehmbares Risiko ist verboten, hohes Risiko muss bestimmte Anforderungen erfüllen, begrenztes Risiko hat Transparenzpflichten.

Innovationsförderung

Der AI Act soll die Entwicklung und den Einsatz von KI-Systemen in der EU fördern.

Aufsicht & Sanktionen

Aufsichtsbehörden überwachen die Einhaltung und können bei Verstössen Sanktionen verhängen.

SWISS INFOSEC

VIELEN
DANK

MELDEN SIE SICH JETZT AN FÜR DIE KOSTENLOSE FACHVERANSTALTUNG

MEET SWISS INFOSEC!
Sicherheit im Fokus

Zürich Flughafen
13 bis 17 Uhr, anschliessend Apéro
www.infosec.ch/msi

Haben Sie schon den kostenlosen
Newsletter abonniert?
www.infosec.ch/news