SEQIS QualityNews

AI. Analysis. Development. Test. Management

Ausgabe H1/2026

Digital Trust: Warum Qualität die neue Währung ist

Quality Assurance als Vertrauensanker: Warum Testen mehr ist als Fehlersuche — Seite 4

Europas Dritter Weg: Die EU-Architektur für eine sichere und faire Digitalisierung — Seite 32

Datensouveränität in Zeiten generativer KI: Warum nur eine lokale Lösung die richtige Antwort ist — Seite 46

Bild generiert von Gemini (Google AI)

AI. Analysis. Development. Test. Management. Better Results.

Lesen Sie in dieser Ausgabe:

Editorial.....3

Quality Assurance als Vertrauensanker: Warum Testen mehr ist als Fehlersuche.....4
Tanja Huber

Compliance & Regulation: Was der EU AI Act für die Softwareentwicklung bedeutet.....6
Martin Brandhuber

Testautomatisierung, KI und externe Testunterstützung: Warum KI und Testing-Tools alleine nicht reichen.....10
Alexander Vukovic

Vom vermeintlichen Bremsklotz zum Gütesiegel: Wie der EU AI Act Qualität zur härtesten Währung macht.....15
Alexander Lewisch

Testautomatisierung – Segen oder Risiko? Warum nur validierte Tests echtes Vertrauen schaffen.....20
Ahmed Soliman

Mobile App Testing: Vertrauen in der Hosentasche – Qualität für die Welt der Endgeräte.....22
Tanja Huber

Qualitätssicherung „as a Service“: Warum externe Expertise die Objektivität und damit das Vertrauen stärkt.....24
Eric Pieber

Vom Bug-Reporting zum Quality Consulting: Warum Beratung der nächste Schritt nach dem Finden von Fehlern ist.....28
Fatemeh Ghaffaari

Europas Dritter Weg: Die EU-Architektur für eine sichere und faire Digitalisierung.....32
Alexander Lewisch

Vertrauen & radikale Transparenz als härteste Währung im ITProjektmanagement.....42
Melanie Gau

Datensouveränität in Zeiten generativer KI: Warum nur eine lokale Lösung die richtige Antwort ist.....46
Alexander Vukovic

AI Development mit Qualität und Bewusstsein.....51
Klemens Loschy

Warum digitales Vertrauen mit der Business Analyse beginnt.....54
Melanie Gau

Über SEQIS QualityNews:

Dieses Magazin richtet sich an Gleichgesinnte aus den Bereichen IT Analyse, Development, Softwaretest und Projektmanagement im IT Umfeld. Die SEQIS Experten berichten über ihre Erfahrungen zu aktuellen Themen in der Branche. Die Leser des Magazins gestalten die Ausgaben mit: Schreiben Sie uns Ihre Meinung im SEQIS Blog (www.SEQIS.com/de/blog-index) oder als Leserbrief.
Wenn Sie dieses Magazin abbestellen möchten, senden Sie bitte ein Mail an marketing@SEQIS.com.

Impressum:
Information und Offenlegung gem. §5 E-Commerce-Gesetz und §25 Mediengesetz

Herausgeber: SEQIS Group GmbH, Wienerbergstraße 3-5, A.1100 Wien
info@SEQIS.com, www.SEQIS.com
Gericht: Handelsgericht Wien
Firmenbuchnummer: 639037k
Umsatzsteuer-ID: ATU81325978
Geschäftsführung: Mag. (FH) Alexander Vukovic, Mag. (FH) Alexander Weichselberger, Manfred Schützhofer, BSc., Klemens Loschy

Druck: druck.at Druck- und Handelsgesellschaft mbH, 2544 Leobersdorf
Erscheinungsweise: 2x pro Jahr

Mag. Alexander Weichselberger | Klemens Loschy | DI Reinhard Salomon | Manfred Schützhofer, BSc | Mag. Alexander Vukovic

Editorial

Sehr geehrte Leserin,
sehr geehrter Leser,

wir freuen uns, Ihnen die Ausgabe für das erste Halbjahr 2026 zu präsentieren.

Vielen Dank für das positive Feedback zu unserer letzten Ausgabe zu dem Themenbereich „AI Act & Local AI - Wege in eine verantwortungsvolle Zukunft". Wir hoffen, wir konnten Ihnen damit interessanten Content zur Verfügung stellen und Sie stellenweise auch gut unterhalten. Über weitere Anregungen, Themenwünsche und Feedback Ihrerseits freuen wir uns.

Auch in dieser Ausgabe finden Sie neben den branchenbezogenen Artikeln auch nicht-technische Bereiche:

In dieser Ausgabe dreht sich alles um das Thema „Digital Trust Warum Qualität die neue Währung ist". Wie immer bieten wir eine Auswahl von Fachartikeln mit diesem Schwerpunkt, die wir aus unserem blog.seqis.com für Sie zusammengestellt haben.

Auf den folgenden Seiten geben Ihnen unsere Experten einen Einblick in die vielseitigen Aspekte zum Thema.

Wir wünschen Ihnen viel Lesevergnügen mit der aktuellen Ausgabe der SEQIS QualityNews!

Ihre SEQIS Geschäftsleitung

Quality Assurance als Vertrauensanker: Warum Testen mehr ist als Fehlersuche

von Tanja Huber

Quality Assurance, im Deutschen "Qualitätssicherung" (folglich abgekürzt mit QA), wird oft fälschlicherweise als reine Fehlersuche angesehen. Am Ende eines Projektes kommt der Tester, prüft das Produkt auf Herz und Nieren und segnet es nach getaner Arbeit ab. Wahre QA ist aber weit mehr als das einfache Aufspüren von Bugs, Fehlern und Fehlzuständen. Sie ist auch keinesfalls erst am Ende eines Projektes. Zunächst einmal sehen wir uns die aktuelle Definition von Qualitätssicherung gemäß ISTQB an.

Aktivitäten, die darauf fokussieren, Vertrauen in die Erfüllung der Qualitätsanforderungen zu erzeugen. [1]

Wir sehen: Schon die offizielle Definition des Begriffs legt fest, dass Quality Assurance darauf abzielt, Vertrauen in Qualität zu schaffen. Bereits in ihrer Definition soll QA ein Vertrauensanker sein. Diese Rolle wird vom Tester übernommen. Doch wie genau wird dieses Vertrauen aufgebaut? Der folgende Artikel beleuchtet diese Frage.

Was macht ein Tester überhaupt? Und wie hat sich das Bild des Testers im Laufe der Jahre geändert?

Gemäß ISTQB ist die Rolle des Software-Testers das Evaluieren von Arbeitsergebnissen gemäß Anforderungen, das Finden von Fehlern, das Verringern von Risiken einer unzureichenden Softwarequalität, das Verifizieren bezüglich rechtlicher Rahmenbedingungen und… vor allem: Das Aufbauen von Vertrauen in die Qualität der Software. Denn: Testen (an der richtigen Stelle eingesetzt) ist ein kosteneffizientes Mittel, Fehlerzustände zu entdecken und zu beseitigen, bevor sie zu einem Problem werden können. Mittels der Planung, der Erstellung und der Durchführung von Tests kann ein Tester diese Aufgaben erfüllen.

Vom Bug-Jäger zum Informationslieferanten

Abbildung 1: Dramatisierung eines traditionellen Testers
Quelle: Von der Autorin gezeichnet

Traditionell wurde der Tester oft als bloßer „Gatekeeper" am Ende der Kette gesehen – ein Hindernis, das Fehler findet und kurz vor dem Release für Stress sorgt. Doch dieser Fokus auf reine Fehlersuche ist schwer messbar und sagt wenig über die eigentliche Produktgüte aus.

Das Bild und die Rollen und Aufgaben eines Testers haben sich gewandelt. Das Stichwort ist "Shift Left". Der moderne Tester begleitet von Beginn an alle Phasen mit und trägt aktiv zur Sicherung hoher Qualität bei. Fehler sollen vermieden werden, statt sie später erst zu finden. Dadurch können potenzielle Fehler frühzeitig identifiziert und behoben werden - noch bevor sie in den Code einfließen.

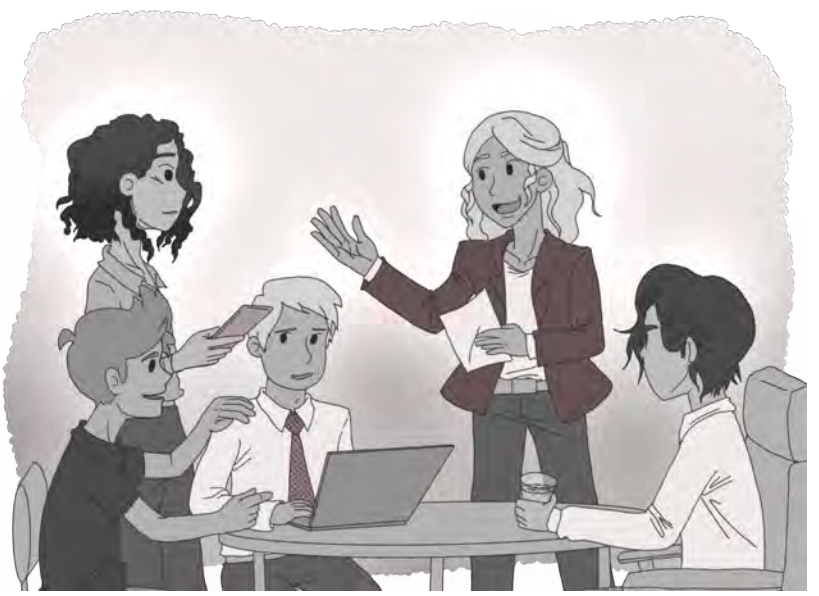


Abbildung 2: Quality Assurance ist Teamarbeit - Alle tragen zum Erfolg bei
Quelle: Von der Autorin gezeichnet

Doch am wichtigsten: In der modernen Wahrnehmung des Rollenbildes eines Testers arbeitet der Tester von Anfang an mit dem gesamten Team zusammen und schafft diverse Präventionen für möglichst wenig Fehler und möglichst hohe Qualität. Das gesamte Team ist für ein erfolgreiches Projekt notwendig und zieht an einem Strang, um ein erfolgreiches Produkt zu erschaffen. Mit regelmäßigen Tests bietet der Tester einen transparenten Einblick in den aktuellen Qualitäts- und Fortschrittsstatus des Produktes oder des Projektes, wodurch auch frühzeitig Gegenmaßnahmen ergriffen werden können, sobald Probleme erkannt werden.

Wie entsteht das Vertrauen? Durch das Mindern von Ungewissheit! Durch Bereitstellen von entscheidenden Informationen!

Ein stabiles Vertrauen entsteht durch die Reduktion von Ungewissheit. Eine vollständige Eliminierung von Risiken ist eine Illusion und wird nie erreichbar sein. Bei der Aufgabe des Testers geht es vielmehr darum, diese Risiken transparent und handhabbar zu machen. Jedes gefundene Risiko liefert wichtige Informationen für fundierte Entscheidungen. Durch die präzise Bewertung dieser Risiken können Projektverantwortliche und das Management entscheiden, ob ein bekanntes Risiko akzeptiert, gemindert, oder durch zusätzliche Entwicklungs- oder Testaufwände beseitigt werden muss oder transferiert werden kann, bevor es zu einem kritischen Vertrauensverlust beim Endnutzer führt. QA ist somit nicht nur ein Kontrollmechanismus, sondern ein integraler Bestandteil der Wertschöpfungskette, der die Zuverlässigkeit und Marktfähigkeit des Produkts direkt beeinflusst.

Des Weiteren liefert QA dem Management eine objektive Entscheidungsgrundlage für beispielsweise Release-Termine. Ein solcher Termin wird nicht mehr durch „Bauchgefühl" und "sollte schon passen" entschieden, sondern durch messbare Fakten (Testabdeckung, Kritikalität und Anzahl offener Fehler, usw.). Das schafft Vertrauen im Management in die Release-Entscheidung.

QA als Vertrauensanker bedeutet letztlich, Unsicherheit durch Wissen zu ersetzen. Für das Management bedeutet das: Weg vom riskanten Hoffen, hin zu einer fundierten Release-Entscheidung basierend auf echten Daten. Für das Team bedeutet es: Die Sicherheit, dass mutige Innovationen durch ein stabiles Qualitätsnetz abgesichert sind. Und für den Endbenutzer, dass ein funktionierendes Produkt zur Verfügung steht. So wird QA zum Fundament, auf dem alle Beteiligten – vom Entwickler bis zum Endanwender – stabil stehen können.

Quellen und weiterführende Informationen:

[1] https://glossary.istqb.org/de_DE/term/qualitatssicherung

https://www.austriantestingboard.at/wp-content/uploads/2023/09/CTFL_Lehrplan_DE.pdf

Ein besonderes Highlight:

Alle Abbildungen dieses Beitrags wurden mit viel Talent und Hingabe von der Autorin selbst entworfen und gezeichnet.

Tanja Huber ist Consultant bei SEQIS.

Zusätzlich zu ihrer Erfahrung in den Bereichen Testfallerstellung, Testdurchführung und Testunterstützung ist sie auch in den Bereichen Projekt- und Qualitätsmanagement tätig.

Beim Herangehen an neue Aufgaben ist ihr eine gewissenhafte Vorgehensweise und kreative Aufgabenlösung wichtig. Ebenso legt sie größten Wert auf hochwertige Qualitätssicherung.

Compliance & Regulation: Was der EU AI Act für die Softwareentwicklung bedeutet

von Martin Brandhuber

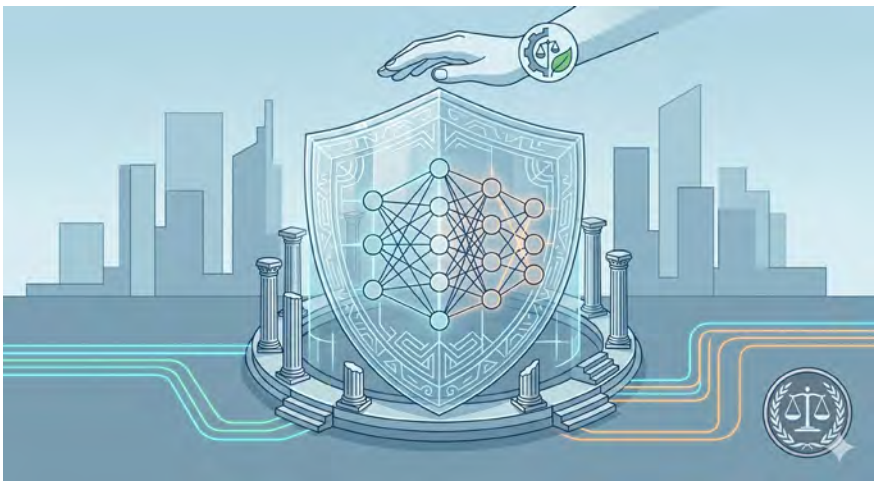


Abbildung 1: Quelle: Bild generiert von Gemini (Google AI)

Der neue Bauplan für die digitale Welt: Wie der EU AI Act die Softwareentwicklung verändert

Immer, wenn ich an die Frühzeit der modernen Tech-Giganten denke, fällt mir das berühmte (und berüchtigte) Motto ein: „Move fast and break things." Einfach mal machen, Code in die Welt pushen und schauen, was passiert. Doch wenn wir uns die rasante Entwicklung der Künstlichen Intelligenz in den letzten Monaten ansehen, erinnert mich dieses Vorgehen eher an den legendären Satz von Dr. Ian Malcolm (Jeff Goldblum) in Jurassic Park: *„Ihre Leute waren nur darauf konzentriert, ob sie es schaffen können. Ob sie es tun sollten, die Frage stellte sich keiner."* Künstliche Intelligenz hat die Laborphase längst verlassen. Und genau hier greift nun der EU AI Act ein – der weltweit erste umfassende Versuch, der KI quasi die von Isaac Asimov erdachten Robotergesetze für das 21. Jahrhundert aufzuerlegen. Für uns in der Softwareentwicklung, im Projektmanagement und im Testing bedeutet das einen massiven Wendepunkt: Recht, Ethik und Code müssen ab sofort Hand in Hand gehen. Gute Compliance ist nicht länger nur ein juristisches Feigenblatt, sondern ein knallhartes Qualitätsmerkmal. Aber was heißt das nun konkret für unseren Entwicklungsalltag?

1. *Die Einordnung: Sag mir, was du tust, und ich sage dir dein Risiko*

Bevor wir künftig auch nur eine einzige Zeile Code in unsere Tastaturen tippen, steht eine neue Hürde ins Haus: die rechtliche Einordnung. Die technische Architektur folgt ab sofort strikt der Regulierung.

Software wird nicht mehr primär nach ihren coolen Features bewertet, sondern nach dem Einsatzkontext. Ein Beispiel: wir bauen eine KI-Bilderkennung. Nichts Weltbewegendes, Standard-Machine-Learning. Wir trainieren das Modell darauf, auf dem Smartphone unsere privaten Urlaubsfotos nach Kategorien wie „Strand" und „Berge" zu sortieren. Rechtlich gesehen? Solche Systeme fallen in die Kategorie „Minimal" oder „Limited Risk". Hier haben wir keine regulatorische Bauchschmerzen, die reine Sortierung macht uns keine Probleme. Als App zur rein persönlichen, nicht-professionellen Nutzung ist das kein Problem. Nehmen wir jetzt aber denselben Algorithmus – dieselben Gewichte im neuronalen Netz, dieselbe Codebase – und setzen ihn zur Überwachung von Mitarbeiter:innen am Arbeitsplatz ein: dann leuchtet sofort die rote Lampe auf - wir haben ein Hochrisiko-KI-System gebaut!

Das Zauberwort für diese neue operative Herausforderung lautet „Compliance by Design". Wir müssen proaktiv prüfen, wo unsere Software landet. Und hier stoßen wir auf das Dilemma des Dual Use. Was, wenn unsere harmlos gedachte Software von User:innen zweckentfremdet wird? Wie ein Küchenmesser, das zum Gemüseschneiden gedacht ist, aber auch als Waffe dienen kann. Wir können nicht jeden Missbrauch vorhersehen, aber die Regulierung zwingt uns, smarte „Guardrails" (technische Leitplanken) in unser Design einzubauen. Wir müssen Software von Beginn an durch die Brille der gesellschaftlichen Verantwortung betrachten. Für den Alltag bedeutet dies: der Zwang zur „Compliance by Design" bedeutet das Ende des reinen Feature-getriebenen Sprints. Rechtliche Anforderungen werden ab sofort Teil der Definition of Done. Ein Ticket kann nicht geschlossen werden, wenn nicht geklärt ist, in welche Risikoklasse das Feature fällt. Security-, Privacy- und nun auch AI-Compliance-Checks rücken im Entwicklungszyklus ganz nach links - das wohlbekannte „Shift-Left".

2. *Daten-Governance: „Garbage In, Lawsuit Out"*

Früher galt im Big-Data-Rausch oft die Devise: Je mehr Daten wir in den Algorithmus pumpen, desto besser. Die Herkunft? Nebensache. Heute weicht dieser wilde Westen der strengen Pflicht zu „Clean & Fair Data".

Nun gibt es klare Grenzen. Es reicht nicht, dass Daten einfach nur „da" sind. Sie müssen repräsentativ, fehlerfrei und – ganz wichtig – auf Biases (Vorurteile) geprüft sein. Wenn wir eine Recruiting-KI fast ausschließlich mit männlichen Lebensläufen trainieren, bauen wir uns schlichtweg einen automatisierten Chauvinisten, der Bewerber:innen anderer Geschlechter systematisch aussortiert. Also sowohl Frauen als auch Personen, die sich als divers, inter, nicht-binär, gender-fluid, agender, pan oder anderen Geschlechtern zugehörig fühlen.

Und: wie misst man ein philosophisches Konzept wie „Fairness" im Code? Hier müssen wir ehrlich sein: Die perfekte, absolut vorurteilsfreie KI gibt es nicht, weil es auch keine absolut vorurteilsfreie Welt gibt, aus der wir die Daten ziehen. Für Data Scientists und QA-Teams geht es künftig um Prozess-Compliance. Sie müssen beweisen, dass sie systematisch nach Biases gesucht und diese minimiert haben (z.B. durch Disparate Impact Ratio oder Equalized Odds). Data Cleaning ist endgültig kein lästiger Anhang mehr, den man Praktikant:innen überlässt. Wer heute unsaubere Daten einspeist, kassiert nicht nur schlechte Ergebnisse, sondern riskiert direkte rechtliche Konsequenzen. Aus Garbage In, Garbage Out wird schlichtweg: Garbage In, Lawsuit Out.

Aber was, wenn die KI beim Training oder im laufenden Betrieb gehackt wird? Wenn absichtlich manipulierte Daten in den Trainingsdatensatz eingeschleust werden? Die Antwort laut AI Act: „Garbage In, Lawsuit Out" bekommt hier eine Security-Dimension. Unternehmen müssen die Resilienz gegen das sogenannte "Data Poisoning" nachweisen. Das erfordert Data Provenance – also eine lückenlose, kryptografisch abgesicherte Nachverfolgung, wer wann welche Daten in den Trainingspool eingespeist hat. Zudem braucht es Algorithmen zur Anomalieerkennung bereits während der Trainingsphase, die statistische Ausreißer im Datensatz automatisch flaggen. Daten-Governance bedeutet unter dem AI Act nicht nur, Daten auf Fairness und Qualität zu prüfen, sondern sie wie hochsensible, geschäftskritische Infrastruktur gegen Sabotage zu härten – sowohl im stillen Kämmerlein des Trainings als auch draußen im Betrieb.

3. Das Ende der „Black Box": Transparenz & Erklärbarkeit

Manche kennen den Sketch aus Little Britain: Ein Kunde fragt nach einem Kredit, sitzt vor einer Bankangestellten, diese tippt lustlos auf ihrer Tastatur herum, starrt auf den Bildschirm und sagt monoton: „Computer says no". Wenn der Kunde dann fragt: „Warum?", weiß das niemand. Weder die Angestellte, noch der Filialleiter, noch der Programmierer.

Genau das darf heute nicht mehr passieren. Wenn eine High-Risk-KI eine Entscheidung trifft, darf dies nicht im Verborgenen eines mysteriösen Algorithmus geschehen - wir sprechen hier von Explainable AI (XAI). Ein System muss nicht nur rasend schnell ein mathematisches Ergebnis ausspucken, sondern auch eine logische Begründung mitliefern, die ein Mensch – oder im Zweifelsfall ein Gericht – nachvollziehen kann. Umfassende Log-Files werden zur Pflicht, genauso wie glasklare „Beipackzettel" für die User:innen, die genau erklären, wo die KI brilliert und wo sie Fehler macht. Bei neuronalen Netzen mit Milliarden von Parametern können wir nicht jede einzelne Berechnung nachvollziehen. Stattdessen nutzt die Industrie Methoden wie SHAP (Shapley Additive exPlanations) oder LIME (Local Interpretable Model-agnostic Explanations). Diese Tools zeigen nicht den exakten Weg des Algorithmus, aber sie visualisieren, welche Input-Faktoren (z. B. das Alter oder das Einkommen in einem Datensatz) den stärksten Einfluss auf die finale Entscheidung hatten.

Hinzu kommt die wichtige Kennzeichnungspflicht im Kampf gegen Deepfakes und Desinformation: Alles, was künstlich generiert wurde (Texte, Chat, Fotos…), muss als KI-Produkt markiert werden.

4. Human-in-the-Loop: Design gegen das blinde Vertrauen

So atemberaubend die technologischen Effizienzgewinne auch sind, der EU AI Act zieht eine rote Linie: in hochsensiblen Bereichen entscheidet die Maschine niemals völlig autonom. Es braucht immer den sogenannten „Human-in-the-Loop". Eine medizinische KI oder eine Kreditvergabe-Software darf nur assistieren, niemals als Alleinentscheider fungieren. Irgendjemand muss den sprichwörtlichen Not-Aus-Schalter in der Hand behalten.

Für unsere UI/UX-Designer:innen ist das eine faszinierende Herausforderung. Wir Menschen neigen aus Bequemlichkeit zum Automation Bias – wir vertrauen dem Computer blind und klicken ungelesen auf „Akzeptieren". Wenn es um Hochrisikosysteme geht, muss das Credo „Don't Make Me Think" von Steve Krug ganz bewusst ausgesetzt werden. Wie bauen wir nun Benutzeroberflächen, die unsere User:innen förmlich dazu zwingen, innezuhalten, kritisch zu denken, und aktiv Verantwortung zu übernehmen? Wir müssen bewusste Reibungspunkte in die Software einbauen, damit der Mensch nicht zum reinen Knöpfchendrücker degradiert wird. Lehnt eine Bankangestellte den KI-Vorschlag ab (oder nimmt ihn unkritisch an), muss sie die Entscheidung z.B. mit einem kurzen Text begründen - das durchbricht das reflexartige Durchklicken. Außerdem: die KI gibt keine absoluten Wahrheiten aus („Das ist ein Betrugsversuch"), sondern Wahrscheinlichkeiten („Zu 82 % eine Anomalie"). Das zwingt den Menschen, die restlichen 18 % mental zu bewerten. Es geht darum, den „Friction-Point" genau dort zu platzieren, wo die kritische Entscheidung

fällt, und den Rest des Workflows weiterhin so flüssig wie möglich zu lassen.

5. *Das Open-Source-Dilemma: Wer haftet für den Code?*

Ein besonders heiß diskutiertes Thema betrifft die Open-Source-Community. Wer zahlt die Zeche, wenn ein offenes KI-Modell von Dritten in eine lukrative kommerzielle App eingebaut wird und dort Schaden anrichtet? Der EU AI Act versucht hier einen Spagat: reine Forschung und Hobby-Entwicklung bleiben weitgehend verschont. Aber sobald aus dem Code ein kommerzielles Produkt wird, schnappt die Haftungsfalle zu.

Software wird heute meist wie bei Lego-Steinen aus bestehenden Modulen zusammengesetzt. Die Rechtslage schützt im Grunde reine Open-Source-Entwicklung. Der Entwickler, der das Modell auf Hugging Face stellt, haftet in der Regel nicht. Aber: sobald du als Unternehmen dieses freie Modell nimmst, es in deine kommerzielle App einbaust und als Hochrisikosystem auf den EU-Markt bringst, wirst du rechtlich zum Betreiber bzw. Anbieter. Die Haftungsfalle schnappt bei dir zu. Du musst die Compliance, die Datenqualität und die Logs für dieses Modell verantworten – egal, wer es ursprünglich geschrieben hat. Also eine Pflicht zur Prüfung der gesamten „Software Supply Chain" auf Altlasten.

Fazit

Ist der EU AI Act nun freudige Zukunftsmusik oder ein Bürokratie-Monster? Müssen wir Angst haben, dass er die europäische Tech-Szene abwürgt? Es wird heftig diskutiert, ob innovative Start-ups nun frustriert ins Ausland abwandern, da sie den Anforderungen des EU AI Acts nicht standhalten können. Doch vielleicht erleben wir auch genau das Gegenteil: Vertrauen wird zur wichtigsten Währung in der KI-Ära. Wenn eine Software das Siegel „EU AI Act Compliant" trägt, wissen Kunden weltweit, dass diese Software auf Sicherheit, Fairness und Transparenz geprüft wurde. Genauso wie die DSGVO heute global als Qualitätsmerkmal für Datenschutz gilt, könnte dieser - zugegeben schmerzhafte - Transformationsprozess Europas Tech-Branche ein entscheidendes Alleinstellungsmerkmal in der Welt verschaffen.

Verordnung (EU) 2024/1689 - EU AI Act

Die Einordnung als erste Hürde
- Unacceptable Risk (Verbote): Artikel 5
- High-Risk (Hochrisiko): Artikel 6 in Verbindung mit Anhang III (Annex III)
- Minimal/Limited Risk: Artikel 50

Daten-Governance (Datenqualität)
- Anforderungen an Daten: Artikel 10

Transparenz & Erklärbarkeit (Black Box)
- Transparenz für Nutzer: Artikel 13 (Informationen für die Betreiber/Deployer)
- Aufzeichnungspflichten (Logging): Artikel 12
- Technische Dokumentation: Artikel 11 und Anhang IV.

Human-in-the-Loop
- Menschliche Aufsicht: Artikel 14

Open Source & Haftung
- Ausnahmen für Open Source: Artikel 2 Absatz 12
- GPAI (General Purpose AI): Artikel 53 und die Erwägungsgründe 102 bis 104

Webcast-Tipp

Martin Brandhuber ist Senior Consultant und Teamlead bei SEQIS.

„Kundenzufriedenheit und Professionalität in der Planung und Durchführung des Testprozesses hat für mich höchste Priorität. Testen ist für mich ein nicht wegzudenkender Bestandteil der Softwareentwicklung. Da die Anforderungen an den Vernetzungsgrad von Systemen laufend zunehmen, ist die frühe Einbindung von Testprozessen in der Softwareentwicklung unabdingbar. Nur so kann die Entwicklung kostengünstiger, qualitativ hochwertiger Software garantiert werden."

Testautomatisierung, KI und externe Testunterstützung: Warum KI und Testing-Tools alleine nicht reichen

von Alexander Vukovic

Abbildung 1: Quelle: Bild generiert von AI

1. Der neue Goldrausch: KI in der Testautomatisierung

Es gibt Phasen in der IT, in denen eine Technologie so dominant wird, dass sie alles andere zu verdrängen scheint. In den 2010er-Jahren war es Agile. Dann kam DevOps. Und jetzt, Mitte der 2020er, erleben wir den KI-Goldrausch in der Testautomatisierung.

Die Versprechen sind verlockend: Generative KI schreibt Unit-Tests in Sekunden. KI-gestützte Tools generieren Playwright-Skripte aus Screenshots. Selbstheilende Testsuiten passen sich automatisch an UI-Änderungen an. Und Reasoning-Modelle analysieren Anforderungen und leiten daraus Testfälle ab, für die ein menschlicher Tester Stunden oder Tage bräuchte.

All das ist real. All das funktioniert. Und all das ist — für sich alleine genommen — **nicht genug.**

Denn zwischen einem funktionierenden KI-Tool und einer funktionierenden Teststrategie liegt ein Abgrund, über den keine noch so schlaue Maschine eine Brücke bauen kann.

Dieser Abgrund heißt: **Kontext, Erfahrung und Urteilsvermögen.**

2. Was KI in der Testautomatisierung heute leistet

Bevor wir kritisch werden, lassen Sie uns anerkennen, was KI bereits heute in der Testautomatisierung leistet — und zwar hervorragend:

Testfallgenerierung: Reasoning-Modelle wie Magistral (Mistral AI) oder Qwen3-Coder-Next können aus User Stories oder Anforderungsdokumenten systematisch Testfälle ableiten. Sie wenden dabei formale Methoden an — Äquivalenzklassenbildung, Grenzwertanalyse, Zustandsübergangsdiagramme — schneller und vollständiger als die meisten menschlichen Tester.

Code-basierte Testautomatisierung: Coding-Modelle wie Devstral 2 generieren Unit-Tests, Integrationstests und API-Tests direkt aus dem Source-Code. Sie verstehen den Kontext ganzer Klassen und Module und können auch Randfall-Tests erzeugen, die ein Entwickler möglicherweise unter Zeitdruck übersehen hätte.

UI-Testautomatisierung: KI-gestützte Tools können Page-Object-Modelle erstellen, Selektoren warten, wenn sich das DOM ändert, und sogar visuelle Regressionen erkennen — Aufgaben, die traditionell extrem wartungsintensiv waren.

Testdatengenerierung: Generative Modelle erzeugen DSGVO-konforme synthetische Testdaten, die semantisch korrekt sind — inklusive konsistenter Adressdaten, plausibler Geburtsdaten und gültiger Prüfziffern (letzteres 100% korrekt dann, wenn deterministische Validierungs-Engines integriert werden).

Log-Analyse und Root Cause Identification: Reasoning-Modelle korrelieren Fehlermeldungen über Microservices hinweg und identifizieren Root Causes, die ein Mensch erst nach stundenlangem Log-Wühlen gefunden hätte.

Diese Fähigkeiten sind beeindruckend. Und sie führen zu einer gefährlichen Schlussfolgerung.

3. Die gefährliche Illusion

Abbildung 2: Quelle: Bild generiert von AI

„KI ersetzt den Tester"
In manchen Unternehmen — insbesondere dort, wo Testing ohnehin als lästige Pflicht wahrgenommen wird — hat sich eine Erzählung etabliert, die ungefähr so klingt:

„Wir haben jetzt Copilot und ein paar KI-Tools. Die generieren uns die Tests. Wir brauchen keine dedizierten Tester mehr. Und externe Unterstützung schon gar nicht."

Diese Erzählung ist verführerisch. Sie verspricht Kosteneinsparung. Sie passt zum Narrativ der technologischen Disruption. Und sie ist grundfalsch.

Hier ist, warum:

KI hat keinen Kontext für Ihr Geschäft
Ein KI-Modell weiß nicht, dass Ihr Versicherungsprodukt „Komfort Plus" seit letztem Quartal andere Deckungsgrenzen hat. Es weiß nicht, dass der Storno-Prozess bei Tarif X eine regulatorische Sonderregelung hat, die im Code als hartkodierte Ausnahme implementiert ist. Es kennt nicht die Geschichte des Systems — warum bestimmte Workarounds existieren, welche Module „Angst-Code" enthalten, den niemand anfasst, und welche Integrationspunkte bei jedem Release wackeln.

Ein erfahrener Testexperte weiß das. Oder er weiß, wie er dieses Wissen systematisch erhebt.

KI generiert Tests — sie bewertet sie nicht
Ein Reasoning-Modell kann 500 Testfälle aus einer Spezifikation ableiten. Aber welche davon sind wichtig? Welche decken die höchsten Risiken ab? Welche sind redundant? Welche passen zur verfügbaren Testzeit? Die Priorisierung von Tests erfordert eine Risikobewertung, die technisches Wissen, Geschäftsverständnis und Projekterfahrung vereint — etwas, das kein Modell leisten kann.

KI automatisiert — sie hinterfragt nicht
Wenn die Anforderung falsch ist, testet die KI die falsche Sache — perfekt automatisiert, aber am Ziel vorbei. Ein erfahrener Tester stellt die Frage: „Ist das wirklich so gemeint? Was passiert, wenn der Benutzer stattdessen X tut?" Diese explorative, hinterfragende Denkweise ist der Kern professionellen Testens — und sie lässt sich nicht automatisieren.

KI erkennt keine organisatorischen Risiken
Die kritischsten Qualitätsrisiken in Softwareprojekten sind oft keine technischen. Sie sind organisatorisch: mangelnde Kommunikation zwischen Teams, unklare Verantwortlichkeiten, Zeitdruck, der zu Abkürzungen führt. Ein externer Testexperte — mit frischem Blick und ohne Betriebsblindheit — erkennt diese Muster. Eine KI nicht.

4. Der Human-in-the-Loop: Nicht optional, sondern essenziell

Der Begriff „Human-in-the-Loop" ist in der KI-Diskussion allgegenwärtig, wird aber oft als Formalität verstanden — ein Häkchen für die Compliance-Checkliste. In der Testautomatisierung ist der Human-in-the-Loop keine Formalität. Er ist die **entscheidende Instanz.**

Die Rolle des Testexperten im KI-Zeitalter
Statt monotoner Routinearbeit konzentriert sich der Testexperte auf das, was wirklich zählt:

Teststrategie und Testdesign: Welche Testarten auf welchen Ebenen? Wo lohnt sich Automatisierung, wo ist explorativer Test effektiver? Wie verteilen wir das Testbudget über Unit-, Integrations-, API- und E2E-Tests?

Risikobasierte Priorisierung: Nicht alles, was testbar ist, muss getestet werden. Der Experte bewertet Risiken und fokussiert auf die Bereiche, die bei einem Fehler den größten Schaden verursachen — geschäftlich, regulatorisch oder reputationsmäßig. Qualitätssicherung der KI-Outputs: Die von der KI generierten Testfälle müssen reviewed, ergänzt und korrigiert werden. Wir haben in der Praxis regelmäßig gesehen, dass KI-generierte Tests technisch korrekt, aber fachlich sinnlos sind — oder umgekehrt, dass sie offensichtliche Geschäftsszenarien ignorieren.

Explorative Tests: Die wertvollsten Bugs werden nicht durch automatisierte Tests gefunden, sondern durch erfahrene Tester, die das System bewusst „anders" benutzen als vorgesehen. Session-Based Exploratory Testing bleibt auch 2026 das mächtigste Werkzeug gegen unbekannte Unbekannte.

Testprozess-Orchestrierung: Jemand muss die CI/CD-Pipeline konfigurieren, die Testumgebungen managen, die Testdatenstrategien definieren und die Ergebnisse interpretieren. KI kann Teile davon unterstützen, aber die Verantwortung liegt beim Menschen.

5. Warum externe Testexpertise den Unterschied macht

Und jetzt kommen wir zum dritten Element der Gleichung: der externen Testunterstützung. Denn selbst wenn ein Unternehmen die richtigen KI-Tools hat und den Human-in-the-Loop versteht — fehlt oft eine entscheidende Zutat: **spezialisierte Testkompetenz auf dem neuesten Stand.**

Das Kompetenzproblem

Die meisten Entwicklungsteams haben Entwickler, die „auch testen". Manche haben dedizierte QA-Ingenieure, die sich im Tagesgeschäft auf Regression und Bug-Triage konzentrieren. Aber die Kombination aus **KI-gestützter Testautomatisierung, modernen Frameworks (Playwright, Cypress), agentischen Workflows und risikobasierten Testdesign** erfordert eine Spezialisierung, die in internen Teams selten vorhanden ist.

Warum? Weil sich die Landschaft so schnell verändert. Vor einem Jahr war Selenium noch Standard. Heute ist Playwright der De-facto-Standard für die UI-Testautomatisierung. Vor sechs Monaten kannte kaum jemand Devstral. Heute schreibt es bessere Tests als mancher Senior Developer. Wer nicht täglich in diesem Ökosystem arbeitet, verliert den Anschluss.

Was externe Testexperten mitbringen

Branchenübergreifende Erfahrung: Ein externer Testexperte, der in 20 verschiedenen Projekten gearbeitet hat, bringt Muster-Erkennung mit, die einem internen Team fehlt. Er hat gesehen, wo typische Architekturen brechen, welche Integrationsszenarien kritisch sind und welche Teststrategien in welchen Kontexten funktionieren.

Frischer Blick ohne Betriebsblindheit: Interne Teams entwickeln zwangsläufig blinde Flecken. Sie testen die Features, die sie kennen, auf die Art, wie sie es immer getan haben. Ein externer Experte hinterfragt Annahmen, entdeckt vernachlässigte Testbereiche und bringt neue Perspektiven ein.

State-of-the-Art-Wissen: Bei SEQIS arbeiten wir täglich mit den neuesten Tools und Modellen. Wir haben Hunderte von Stunden damit verbracht, lokale KI-Modelle für Testautomatisierung zu evaluieren, zu optimieren und in Workflows zu integrieren. Dieses Wissen steht unseren Kunden sofort zur Verfügung — ohne monatelange interne Lernkurve.

Skalierbarkeit: Vor einem Release, bei einer Migration oder nach einer Sicherheitslücke brauchen Sie mehr Testkapazität. Und zwar schnell. Externe Spezialisten können innerhalb von Tagen produktiv sein — mit eigenen Tools, eigenen Methoden und eigener KI-Infrastruktur.

6. Das Drei-Säulen-Modell: KI + Mensch + Expertise

Die Zukunft der Testautomatisierung liegt nicht in einer Entweder-Oder-Entscheidung. Sie liegt in einem **Drei-Säulen-Modell**

Abbildung 3 Drei-Säulen-Modell: KI + Mensch + Expertise:
Quelle: Bild generiert von AI

Das Modell kombiniert die Stärken jeder Komponente:

Säule 1: KI-gestützte Automatisierung Lokale KI-Modelle (wie auf der razzfazz.ai Box) übernehmen die repetitiven, datenintensiven Aufgaben: Testfallgenerierung, Code-Review, Testdatenerstellung, Log-Analyse, Regressionstesting. Sie sind die unermüdlichen Arbeiter, die rund um die Uhr produzieren.

Säule 2: Der Testexperte als Dirigent Der menschliche Testexperte orchestriert, priorisiert, hinterfragt und bewertet. Er definiert die Teststrategie, validiert die KI-Outputs, führt explorative Tests durch und stellt sicher, dass das Richtige getestet wird — nicht nur das Offensichtliche.

Säule 3: Externe Spezialisierung Externe Testpartner bringen die Tiefe und Breite der Erfahrung, die ein internes Team nicht aufbauen kann (und nicht aufbauen muss). Sie kennen die neuesten Frameworks, haben die KI-Tools bereits evaluiert und können Testkompetenz skalierbar bereitstellen.

Keine dieser Säulen funktioniert alleine. KI ohne menschliche Steuerung produziert technisch beeindruckende, aber strategisch sinnlose Tests. Menschliche Expertise ohne KI-Unterstützung skaliert nicht. Und interne Teams ohne externe Impulse erstarren in ihren Gewohnheiten.

7. Ein Praxisbeispiel: Die Symbiose in Aktion

Stellen Sie sich ein mittelständisches Unternehmen vor, das eine Legacy-ERP-Anwendung modernisiert. Bisher wurde manuell getestet — Excel-Listen, Klick-für-Klick, 200 Testfälle vor jedem Release.

Phase 1 — Analyse (Externer Testexperte): Ein SEQIS-Consultant analysiert die bestehende Testlandschaft, identifiziert die risikoreichsten Module und definiert eine Teststrategie. Ergebnis: Ein priorisierter Automatisierungsplan, der zeigt, wo sich Automatisierung lohnt und wo explorativer Test effizienter bleibt.

Phase 2 — Automatisierung (KI + Experte): Auf der razzfazz.ai Box generiert Devstral 2 Playwright-Tests für die identifizierten Kernszenarien. Der Testexperte reviewed jeden generierten Test, ergänzt fehlende Geschäftslogik-Validierungen und baut ein stabiles Page-Object-Modell auf.

Phase 3 — Betrieb (Internes Team + KI): Das interne Team übernimmt die Wartung der automatisierten Tests, unterstützt durch die Self-Healing-Fähigkeiten der lokalen KI. Devstral schlägt bei UI-Änderungen automatisch angepasste Selektoren vor. Magistral generiert Testdaten für neue Features.

Phase 4 — Continuous Improvement (Externer Impuls): Quartalsweise reviewt der SEQIS-Consultant die Teststrategie, identifiziert Lücken und integriert neue Modelle oder Techniken. Er bringt Erfahrungen aus anderen Projekten ein und stellt sicher, dass die Teststrategie mit der Geschäftsentwicklung Schritt hält. Das Ergebnis: **80% der Regressionstests automatisiert**, Release-Zyklen von monatlich auf wöchentlich verkürzt, Testabdeckung verdreifacht — und trotzdem werden die wirklich kritischen Fehler durch explorative Tests von erfahrenen Experten gefunden, nicht von der KI.

Abbildung 4 Praxisbeispiel Timeline: 4 Phasen der Symbiose:
Quelle: Bild generiert von AI

8. Fazit: Die KI ist das Werkzeug — nicht der Meister

Die Verführung ist groß, Testing vollständig an KI-Tools zu delegieren. Die Tools sind gut. Sie werden immer besser. Aber sie bleiben Werkzeuge. Und ein Werkzeug — egal wie scharf — ersetzt nicht den Handwerker, der weiß, wo man schneiden muss.

In einer Welt, in der Software immer komplexer wird, regulatorische Anforderungen steigen und die Kosten von Qualitätsmängeln explodieren, brauchen wir nicht weniger Testexpertise — wir brauchen andere Testexpertise. Experten, die KI-Tools orchestrieren statt sie zu fürchten. Die Teststrategien definieren statt nur Tests auszuführen. Die den Unterschied kennen zwischen „alle Tests grün" und „die Software funktioniert wirklich."

Und wir brauchen externe Partner, die dieses Wissen mitbringen — aktuell, branchenübergreifend und auf den neuesten Stand der Technik. Nicht als Ersatz für das interne Team, sondern als Verstärkung. Als den entscheidenden Unterschied zwischen „wir testen" und „wir sichern Qualität."

KI liefert die Geschwindigkeit.

Der Mensch liefert das Urteilsvermögen.

Externe Expertise liefert die Tiefe.

Zusammen ergeben sie Qualität.

Quellen und weiterführende Informationen:

QualityNews H2/2025 – AI Act & Local AI
https://seqis.com/

razzfazz.ai – Lokal. Open Source. Unabhängig. Sicher.
https://razzfazz.ai/

ISTQB Foundation Level Syllabus v4.0
https://www.istqb.org/

Playwright – Modern web testing
https://playwright.dev/

Mistral AI – Devstral & Magistral
https://mistral.ai/

Session-Based Test Management (SBTM), Jonathan Bach
https://www.satisfice.com/

Podcast-Tipp

www.SEQIS.com

Alexander Vukovic ist SEQIS Gründer und Chief Evangelist.

Er ist erster Ansprechpartner für alle agilen, testmethodischen und testtechnischen Anfragen. In der Praxis arbeitet er als AI Quality Coach, Berater, Interims-Testmanager, CI-Experte und Lasttester. Mehr als 25 Jahre Beratertätigkeit führten ihn während seiner zahlreichen Projekte in die unterschiedlichsten Branchen und Länder. Sein persönliches Motto: „Es gibt keine Probleme, sondern nur nicht gefundene Lösungen."

Vom vermeintlichen Bremsklotz zum Gütesiegel: Wie der EU AI Act Qualität zur härtesten Währung macht

von Alexander Lewisch

Abbildung 1: Quelle: Bild generiert von Gemini (Google AI)

Warum Compliance keine reine Pflichtübung ist, sondern das Fundament für Digital Trust in einer KI-geprägten Welt

Einleitung - Die informationstechnische Notwendigkeit von „Digital Trust“

Die rasante Verbreitung generativer und prädiktiver KI-Systeme in den operativen Geschäftsalltag hat die informationstechnischen Paradigmen der letzten Jahre grundlegend verschoben. Während in der frühen Phase der KI-Adaption primär die algorithmische Leistungsfähigkeit (Performance) im Fokus der Entwicklung stand, zeigt die empirische Akzeptanzforschung mittlerweile ein differenzierteres Bild. Die rein technische Kapazität eines Systems ist keine hinreichende Bedingung für dessen nachhaltige Nutzung. Modelle wie das Technology Acceptance Model (TAM) belegen, dass bei komplexen, nicht-deterministischen Systemen das Konstrukt „Vertrauen“ als essenziell vermittelnde Variable fungiert. Wenn Nutzer und Stakeholder die Entscheidungsprozesse eines Algorithmus als intransparent wahrnehmen, sinken die wahrgenommene Nützlichkeit und damit die Nutzungsintention drastisch. Digital Trust ist somit keine bloße Marketingmetapher, sondern eine quantifizierbare Prämisse für die Technologieakzeptanz.[1]

In diesem kritischen Stadium der Technologieentwicklung greift der EU AI Act als regulatorischer Mechanismus ein. In der öffentlichen und oft populärwissenschaftlichen Debatte wird die Verordnung häufig als innovationshemmende Restriktion wahrgenommen. Da es Anwendern aufgrund der enormen Komplexität unmöglich ist, die Sicherheit und Fairness eines Modells selbst zu evaluieren, etabliert der Gesetzgeber Vertrauen auf institutionalisierter Ebene. Der AI Act fungiert somit nicht als Bremsklotz, sondern als stabilisierendes Element für ein drohendes Marktversagen im KI-Bereich.[2]

Unternehmen, die sich proaktiv an diesen Vorgaben ausrichten, transformieren Compliance von einer reinen Pflichtübung in einen strategischen Enabler. Die rechtlichen Anforderungen zwingen Organisationen zur Implementierung rigoroser IT-Governance-Strukturen, die weit über die gesetzlichen Mindeststandards hinaus betriebswirtschaftlichen Mehrwert generieren. Digital Trust wird zur „License to Operate“ in einer zunehmend automatisierten Wirtschaft, in der nachweisbare Software- und Datenqualität zur neuen Leitwährung avanciert.[3]

Der AI Act als ganzheitliches Framework für Software-Qualität

Bei einer rein juristischen Auslegung des EU AI Acts stehen Strafzahlungen, Risikoklassifizierungen und Dokumentationspflichten im Vordergrund. Überträgt man den Verordnungstext jedoch in die Domäne des Software Quality Engineering (SQE), so lässt er sich als detailliertes Framework für die Entwicklung und den Betrieb komplexer IT-Systeme lesen. Die Verordnung kodifiziert im Wesentlichen Best Practices der Softwarearchitektur für Systeme, die auf stochastischen statt auf deterministischen Prinzipien beruhen. Die Erwägungsgründe des Gesetzes korrespondieren dabei stark mit etablierten internationalen Normen, wie der ISO/IEC 25010 (System- und Software-Qualitätsmodelle) sowie spezifischen Standards für vertrauenswürdige AI, wie der ISO/IEC TR 24028 (vertrauenswürdige AI-Systeme). Der AI Act schließt damit die methodische Lücke zwischen agiler Softwareentwicklung und den Notwendigkeiten eines hochgradig verlässlichen IT-Betriebs.

Das Fundament der Qualitätsarchitektur bildet die Daten-Governance, die durch den AI Act von einer administrativen Empfehlung in den Rang einer rechtlich bindenden Voraussetzung erhoben wird. Da die Performanz von Machine-Learning-Modellen direkt mit der Beschaffenheit

ihrer Trainingsdaten korreliert (Güte der Datensätze), fordert das Gesetz den Nachweis statistischer Repräsentativität und systematischen Bias-Managements (z.B. Disparate Impact Ratio, Statistical Parity). Dies zwingt IT-Abteilungen zur Etablierung durchgängiger Datenanalyse sowie valider Metadaten-Strukturen. Die Sicherstellung der Datenqualität wird somit zur unerlässlichen Bedingung für die rechtmäßige Inbetriebnahme von Hochrisiko-AI-Systemen und gleichzeitig zum effektivsten Instrument zur Minimierung algorithmischer Fehlentscheidungen. In einem Marktumfeld, in dem zahlreiche Anbieter AI-Lösungen implementieren, ist die tatsächliche Systemgüte für den Endkunden vorab verdeckt. Die stringente Konformität mit dem AI Act sowie die damit verbundene nachweisbare Exzellenz in der Software- und Datenqualität fungieren als starkes, glaubwürdiges Signal an den Markt. Es differenziert seriöse von qualitativ minderwertigen Anbietern und macht Qualität zu jenem Gütesiegel, das langfristig den Markterfolg sicherstellt und das Vertrauen von Stakeholdern und Regulierungsbehörden sichert.[4]

Die 3 Säulen des Vertrauens

Der Übergang von abstrakten normativen Anforderungen zu konkreten informationstechnischen Prozessen erfordert eine systematische Operationalisierung des Konstrukts „Vertrauen". In der wissenschaftlichen Literatur zu soziotechnischen Systemen wird Vertrauen in künstliche Intelligenz maßgeblich durch die Dimensionen Verlässlichkeit, Erklärbarkeit und Kontrollierbarkeit determiniert. Der EU AI Act transformiert diese abstrakten ethischen Postulate in messbare technische Standards. Für die IT-Praxis bedeutet dies die Implementierung von drei zentralen Säulen, die das Fundament für rechtskonforme und vertrauenswürdige KI-Systeme bilden.[5]

Abbildung 2: Quelle: Bild generiert von Gemini (Google AI)

Säule 1: Datenintegrität

Die Basis jedes maschinellen Lernmodells bilden dessen Trainings-, Validierungs- und Testdaten. Der Artikel 10 des AI Acts spezifiziert strenge Anforderungen an die Daten-Governance für Hochrisiko-Systeme. Die Qualitätssicherung darf sich nicht länger auf rein syntaktische Prüfungen beschränken, sondern muss semantische und statistische Integrität gewährleisten. Dies umfasst die systematische Untersuchung auf Verzerrungen (Bias) sowie die Sicherstellung der Repräsentativität der Datensätze im Hinblick auf den intendierten Anwendungskontext.[6] Aus wissenschaftlicher Sicht ist bekannt, dass algorithmische Diskriminierung zumeist auf die Unausgewogenheit in den Trainingsdaten zurückzuführen ist. Die proaktive Datenpflege und die Etablierung robuster Datenkonzepte avancieren somit von einer administrativen Aufgabe zur juristisch bindenden Grundvoraussetzung für das Vertrauen in die Technologie.[7]

Säule 2: Menschliche Aufsicht

Technologische Autonomie findet im regulatorischen Rahmen des AI Acts klare Grenzen. Unter dem Paradigma der menschlichen Aufsicht (Art. 14 AI Act) fordert der Gesetzgeber zwingend die Implementierung von Mensch-Maschine-Schnittstellen (Human-in-the-Loop), die es menschlichen Akteuren ermöglichen, in den Entscheidungsprozess der KI einzugreifen, diesen zu überstimmen oder das System im Notfall vollständig zu deaktivieren.[6] In der Disziplin der Mensch-Computer-Interaktion wird dieser Ansatz als „Human-Centered AI" bezeichnet. Er zielt darauf ab, die Leistungsfähigkeit der Algorithmen mit menschlicher Urteilskraft und moralischer Verantwortlichkeit zu fusionieren. Die IT-Architektur muss folglich so konzipiert sein, dass sie nicht nur Entscheidungen automatisiert, sondern dem menschlichen Operator kontinuierlich kontextuelle Situationswahrnehmung (Situation Awareness) ermöglicht.[8]

Säule 3: Nachverfolgbarkeit und Aufzeichnungspflichten

Vertrauen in komplexe IT-Systeme erfordert zwingend algorithmische Verantwortlichkeit. Diese lässt sich nur realisieren, wenn Systementscheidungen nachträglich rekonstruierbar bleiben. Der AI Act manifestiert diese Anforderung in Artikel 12. IT-Systeme müssen mit umfassenden Logging-Mechanismen ausgestattet werden, die eine lückenlose Nachverfolgbarkeit von Inputs, Modellaktivitäten und Outputs gewährleisten. Diese automatisierten Protokolle dienen im Falle von Systemfehlern oder Audits als entscheidendes forensisches Beweismaterial.[6] Die wissenschaftliche Debatte verdeutlicht, dass erst die

methodische Auditierbarkeit die Transformation von einer Black Box zu einem transparenteren und akzeptierten Werkzeug ermöglicht.[9]

Qualität als Wettbewerbsvorteil
Die Implementierung der vom AI Act geforderten Qualitätsstandards ist zweifelsohne mit initialen Transaktions- und Opportunitätskosten verbunden. Reduziert man die Verordnung jedoch auf diese reine Kostenperspektive, verkennt man die fundamentale Informationsökonomie des europäischen Binnenmarktes. Eine unzureichende Daten- und Systemqualität gefährdet die Realisierung dieses Potenzials aber massiv. Der Wissenschaftliche Dienst des Europäischen Parlaments (EPRS) hat in einer weitreichenden Analyse quantifiziert, dass das Fehlen von Vertrauen und fragmentierte Regeln die Wirtschaft Milliarden kostet. Im Umkehrschluss kann ein einheitlicher, ethisch fundierter Qualitäts- und Rechtsrahmen für KI das europäische Bruttoinlandsprodukt bis 2030 um bis zu 294 Milliarden Euro steigern. Dieses ökonomische Potenzial lässt sich jedoch nur heben, wenn IT-Systeme fehlerfrei skalieren.[10] In stochastischen Machine-Learning-Modellen potenzieren sich qualitative Mängel drastisch. Was in der aktuellen AI-Forschung als Daten-Kaskade (Data Cascade) bezeichnet wird, beschreibt das Phänomen, bei dem marginale Fehler im Trainingsdatensatz exponentiell anwachsen und den operativen Output unbrauchbar machen.

Wenn KI-Systeme in kritischen Geschäftsprozessen eingesetzt werden, ist das Vertrauen der Endanwender

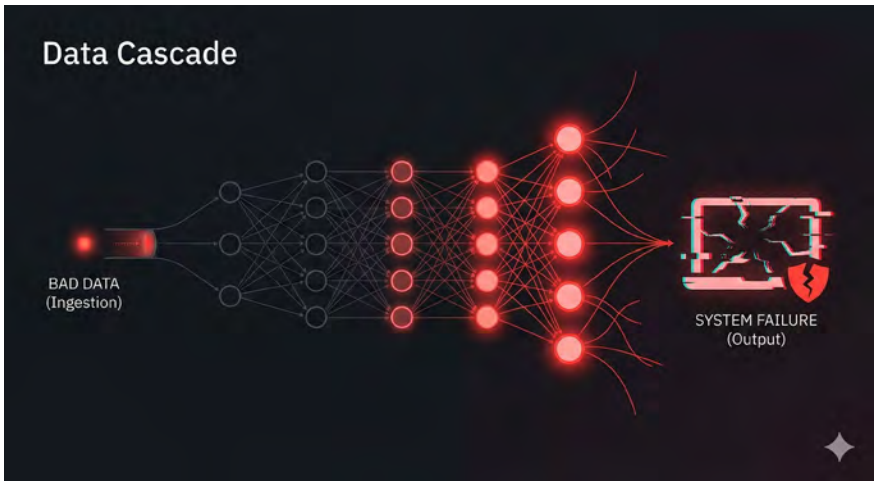


Abbildung 3: Quelle: Bild generiert von Gemini (Google AI)

und Stakeholder die einzige Währung, die eine Skalierung ermöglicht. Eine nachweisbare Konformität mit dem AI Act signalisiert dem Markt eine institutionalisierte Zuverlässigkeit. Compliance wird somit von einer regulatorischen Steuer zur strategischen Investition in den Vertrauensaufschlag („Trust Premium"), der die Marktfähigkeit europäischer AI-Lösungen überhaupt erst garantiert.[11]

Fazit: Der Paradigmenwechsel zu „Trust by Design"
Die Ära der unregulierten und rein explorativen AI-Entwicklung nähert sich ihrem Ende. Der EU AI Act markiert keinen singulären bürokratischen Akt, sondern den Beginn einer neuen Reifephase in der Softwaretechnik. Für IT-Entscheider, CIOs und Data Scientists bedeutet dies einen zwingenden methodischen Paradigmenwechsel von einer nachträglichen, reaktiven Qualitätssicherung hin zu einem proaktiven Konstruktionsprinzip, genannt "Trust by Design". Dieses Konzept fordert die strukturelle Integration menschlicher Werte, rechtlicher Normen und technischer Robustheit bereits in der Anforderungsanalyse eines IT-Projekts. Vertrauen lässt sich nicht nachträglich durch ein Software-Update in ein undurchsichtiges neuronales Netz „patchen".[12]

Der vermeintliche Bremsklotz EU AI Act zwingt die europäische Wirtschaft zur informationstechnischen Exzellenz. In einer zunehmend automatisierten Welt, in der Algorithmen essenzielle Entscheidungen treffen, reicht bloße Funktionalität nicht mehr aus. Digital Trust ist die Lizenz zur Marktteilnahme, und nachweisbare Qualität ist die harte Währung, mit der sie bezahlt wird. Die IT-Abteilungen der Zukunft sind nicht länger nur die Lieferanten von Rechenleistung und Features, sie wandeln sich gerade zu den institutionellen Garanten von Vertrauen.

Podcast-Tipp

Quellen:

[1] Siau, Keng; Wang, Weiyu (2018): Building Trust in Artificial Intelligence, Machine Learning, and Robotics. Cutter Business Technology Journal, 31(2), 47-53. In: https://www.cutter.com/article/building-trust-artificial-intelligence-machine-learning-and-robotics-498981

[2] Veale, Michael; Borgesius, Frederik J. Zuiderveen (2021): Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, 22, 97 - 112. DOI: 10.9785/cri-2021-220402

[3] Mökander, Jakob; Morley, Jessica; Taddeo, Mariarosaria & Floridi, Luciano (2021): Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations. Science and Engineering Ethics, 27(44). DOI: 10.1007/s11948-021-00319-4

[4] Gudivada, Venkat N.; Apon, Amy & Ding, Junhua (2017): Data Quality Considerations for Big Data and Machine Learning: Going Beyond Data Cleaning and Transformations. International Journal on Advances in Software, 10(1&2), 1-20. In: https://personales.upv.es/thinkmind/dl/journals/soft/soft_v10_n12_2017/soft_v10_n12_2017_1.pdf

[5] Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz (2019): Ethik-Leitlinien für eine vertrauenswürdige KI. Europäische Kommission. In: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-de

[6] Europäische Union (2024): Verordnung (EU) 2024/1689 (EU AI Act). Amtsblatt der Europäischen Union. In: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32024R1689

[7] Mehrabi, Ninareh; Morstatter, Fred; Saxena, Nripsuta; Lerman, Kristina & Galstyan, Aram (2021): A Survey on Bias and Fairness in Machine Learning. ACM Computing Surveys, 54(6), Article 115, 1-35. DOI: 10.1145/3457607

[8] Shneiderman, Ben (2020): Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy. International Journal of Human–Computer Interaction, 36(6), 495-504. DOI: 10.1080/10447318.2020.1741118

[9] Mittelstadt, Brent Daniel; Allo, Patrick; Taddeo, Mariarosaria; Wachter, Sandra & Floridi, Luciano (2016): The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1-21. DOI: 10.1177/2053951716679679

[10] Evas, Tatjana (2020): European framework on ethical aspects of artificial intelligence, robotics and related technologies - European added value assessment. Study published by European Parliamentary Research Service (EPRS). In: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654179/EPRS_STU(2020)654179_EN.pdf

[11] Sambasivan, Nithya; Kapania, Shivani; Highfill, Hannah; Akrong, Diana; Paritosh, Praveen & Aroyo, Lora M (2021): "Everyone wants to do the model work, not the data work": Data Cascades in High-Stakes AI. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI 21), 39, 1-15. DOI: 10.1145/3411764.3445518

[12] Merchán-Cruz, Emmanuel A.; Gabelaia, Ioseb; Savrasovs, Mihails; Hansen, Mark F.; Soe, Shwe; Rodriguez-Cañizo, Ricardo G. & Aragón-Camarasa, Gerardo (2025): Trust by Design: An Ethical Framework for Collaborative Intelligence Systems in Industry 5.0. Electronics, 14(10), 1952. DOI: 10.3390/electronics14101952

Weiterführende Informationen

ISO/IEC 25010:2023 (Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model) - Leseprobe: siehe https://www.iso.org/obp/ui/en/#iso:std:78176:en

ISO/IEC TR 24028:2020 (Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence) - Leseprobe: siehe https://www.iso.org/obp/ui/en/#iso:std:77608:en

Alexander Lewisch ist Consultant bei SEQIS.

Als IT-Quereinsteiger und Wiedereinsteiger konnte er Erfahrungen im Software Testing sammeln und Einblicke in diverse Bereiche wie Testmanagement, Testdurchführung, Testautomation, Testkoordination, Reporting und Consulting sammeln.

Derzeit widmet er sich verschiedenen Testprojekten im Bereich der Remote Testing Services (RTS).

Testautomatisierung – Segen oder Risiko? Warum nur validierte Tests echtes Vertrauen schaffen

von Ahmed Soliman

Als Test Automation Engineer höre ich oft denselben Satz: „Wir haben 500 automatisierte Tests – wir sind gut abgesichert." Klingt beruhigend. Aber stimmt es wirklich? Diese quantitative Sicherheit ist trügerisch.

Das Problem mit unkontrollierten Tests

Automatisierte Tests sind kein Selbstzweck. Sie sind ein Werkzeug. Und wie jedes Werkzeug können sie falsch eingesetzt werden. Ein Test, der immer grün ist – egal was passiert – ist kein Test. Er ist eine Illusion von Sicherheit.

In der Praxis sieht man das oft: Tests, die aufgrund von tautologischen Assertions (z. B. assertTrue(true)) oder fehlenden Validierungslogiken nie fehlschlagen. Tests, die auf veralteten Daten laufen. Tests, die nach einem Refactoring still und leise aufgehört haben, das Richtige zu testen. Man nennt das auch False Pass – der Test sagt: "Alles okay", obwohl es das nicht ist. Und das ist gefährlicher als gar keine Tests.

Was bedeutet „validierter Test" eigentlich?

Ein validierter Test ist ein Test, bei dem man weiß:

- Er testet das Richtige – die fachliche Anforderung, nicht nur zufälligen Code.
- Er ist wartbar – er überlebt kleine Änderungen im Design, ohne sofort zu brechen.
- Er hat einen Verantwortlichen – jemand kümmert sich darum, wenn er rot wird.

Validierung bedeutet nicht, jeden Test manuell zu prüfen. Es bedeutet, einen Prozess zu haben, der sicherstellt, dass die Tests noch zur Realität passen.

Der Unterschied zwischen Quantität und Qualität

Mehr Tests bedeuten nicht automatisch mehr Vertrauen. Ein Team mit 50 sorgfältig validierten Tests agiert mit deutlich höherer Release-Sicherheit als ein Team mit 2.000 Tests, die niemand mehr versteht.. Echtes Vertrauen entsteht durch Transparenz: Ich weiß, was getestet wird, warum es getestet wird und dass das Ergebnis verlässlich ist.

Abbildung 1: Quelle: Bild generiert von Gemini (Google AI)

Praktische Schritte zur Testvalidierung

1. Regelmäßige Test-Reviews – Wie Code-Reviews, aber für die Testlogik. Tests veralten still. Eine Anforderung ändert sich, der Code wird angepasst – aber der Test bleibt unberührt und läuft weiter grün. Deshalb sollten Test-Reviews fester Bestandteil des Entwicklungsprozesses sein, idealerweise im selben Rhythmus wie Sprint-Retrospektiven. Die zentrale Frage dabei: Testet dieser Test noch das, was er testen soll?

2. Test Coverage ≠ Test Quality – Eine Codeabdeckung von 80 % klingt beeindruckend – aber Coverage misst nur, ob eine Zeile ausgeführt wurde, nicht ob das Ergebnis korrekt geprüft wurde. Ein Test ohne aussagekräftige Assertions ist wie ein Sicherheitsgurt ohne Befestigung.

3. Flaky Tests sofort adressieren – Ein Test, der manchmal grün und manchmal rot ist, ohne dass sich etwas geändert hat, ist aktiv schädlich. Er erzeugt Alarmmüdigkeit (Alert Fatigue) – Teams beginnen, rote Tests zu ignorieren, weil sie es gewohnt sind, dass eh nichts passiert." Google hat intern dokumentiert, dass Flaky tests eines der größten Hindernisse für Entwicklerproduktivität sind.

4. Einen Test-Owner definieren – Jeder Test sollte einen nament-

lichen Verantwortlichen haben. Nicht ein Team, eine Person. In der Praxis bedeutet das: Wenn ein Test rot wird, gibt es keine Diskussion darüber, wer sich kümmert.

Fazit

Automatisierte Tests sind ein Segen – aber nur, wenn man ihnen mit gesunder Skepsis begegnet. Erst wenn man sicher ist, dass ein Test im Ernstfall wirklich anschlägt, darf man ihm vertrauen. Alles andere ist Hoffnung, keine Qualitätssicherung.

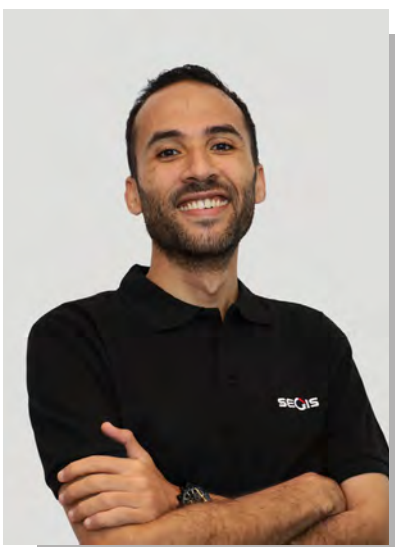
Abbildung 2: Quelle: Bild generiert von Gemini (Google AI)

Quellen und weiterführende Informationen:

ISTQB Glossar: Test Validation & Test Effectiveness – International Software Testing Qualifications Board (ISTQB)

Whittaker, J. (2012). How Google Tests Software. Addison-Wesley.

Beck, K. & Andres, C. (2004). Extreme Programming Explained. Addison-Wesley.



Ahmed Soliman ist Consultant bei SEQIS.

Mit einem Fundament im Maschinenbau und Business Administration fand er seinen Weg in die Welt des Software-Testings und Qualitätsmanagement. Ihn begeistert besonders die Verbindung von technischer Tiefe und strategischer Prozessoptimierung. Seine Schwerpunkte liegen in der Testautomatisierung sowie der Anwendung moderner Tools wie Playwright. Er verfolgt das Ziel, durch kontinuierliche Weiterentwicklung und den Einsatz agiler Methoden die Softwarequalität in funktionsübergreifenden Teams nachhaltig zu steigern.

Mobile App Testing: Vertrauen in der Hosentasche – Qualität für die Welt der Endgeräte

von Tanja Huber

Abbildung 1: Quelle: Bild generiert von Gemini (Google AI)

Heutzutage ist das Smartphone für viele das wichtigste und persönlichste Gerät, das wir besitzen. Der Computer für die Hosentasche ist unser täglicher Begleiter und oft gar nicht mehr aus dem Alltag wegzudenken. Durch den engen Kontakt, den wir tagein, tagaus mit unseren Smartphones pflegen, ist die Sichtbarkeit von Fehlern entsprechend hoch. Saugt eine App in Sekundenschnelle den Akku leer, wird diese App nicht lange auf dem Gerät installiert bleiben. Dementsprechend ist die Qualitäts-Messlatte in der mobilen Welt höher als überall sonst.

Ein wichtiger Aspekt sind die vielfältigen Erwartungen an die Nutzung von Apps. Zum Beispiel: Wird die App-Nutzung durch einen eingehenden Anruf unterbrochen, erwarten Anwender in der Regel, nach dem Anruf an exakt derselben Stelle fortfahren zu können, an der unterbrochen wurde. Wird diese Erwartung erfüllt, resultiert das zwar nicht zwingend in erhöhter Zufriedenheit, aber ihre Nichterfüllung führt mit Sicherheit zu einer negativen Nutzererfahrung. Negative Erfahrungen haben weit mehr Gewicht als positive. Somit sind ausführliche Tests in der mobilen Welt von weitaus größerer Bedeutung, als es auf den ersten Blick erscheinen mag.

Vertrauen durch Verlässlichkeit - Sichergestellt durchs Testen

Beim Mobile App Testing ist es wichtig neben der Software auch die Hardware zu beachten. Angesichts der Vielfalt an Modellen und Funktionen auf dem Markt erwartet jeder Nutzer, dass die Anwendung auf seinem jeweiligen Gerät fehlerfrei funktioniert. Daher liegt einer der Schwerpunkte des Mobile App Testing in der sorgfältigen Auswahl der Testgeräte, um die realen Marktbedingungen so gut wie möglich abzubilden und zu überprüfen. Angesichts der schieren Fragmentierung des Marktes - neben verschiedenen Herstellern gibt es unterschiedliche Bildschirmgrößen und Betriebssysteme und -versionen - ist es technisch und ökonomisch unmöglich, die Software auf jedem existierenden Gerät zu testen. Deswegen wird, basierend auf den Nutzerdaten der User (oder allgemeinen Statistiken) eine repräsentative Auswahl an Geräten ausgesucht, um so eine maximale Marktabdeckung mit minimalem Aufwand zu gewährleisten. Des Weiteren ist es Aufgabe des Testers, auf die Benutzbarkeit und das User Interface der App zu achten. Es wird sichergestellt, dass die App immer intuitiv angewendet und ohne Wartezeiten verwendet werden kann.

Bei weiteren Tests wird Wert auf eine realitätsnahe Testumgebung gelegt, ergänzend zu einer durchdachten Auswahl an Testgeräten. Mit „sogenannten“ Feldtests wird beispielsweise mit dem Handy unterwegs geprüft, ob die Software unter wechselnden Lichtverhältnissen oder Netzverbindungen unterwegs stets einwandfrei funktioniert. Auch bei starker Lichteinstrahlung sollte der Text am Bildschirm lesbar bleiben und auch bei schnellen Bewegungen in öffentlichen Verkehrsmitteln soll die

mobile Verbindung beziehungsweise die Verwendbarkeit nicht beeinträchtigt werden. Und zu keinem Zeitpunkt sollte der Akku mehr als notwendig beansprucht werden.

Ein besonderer Fokus beim Testen liegt auch auf der Sicherheit der Daten. Es wird sichergestellt, dass die App nur nach den Berechtigungen fragt, die sie auch benötigt und keine unverhältnismäßigen Berechtigungen einfordert. Beispielsweise wird sichergestellt, dass der Zugriff auf das Mikrofon ausschließlich dann stattfindet, wenn es notwendig ist. Es wird zudem gewährleistet, dass die App auch dann einsatzfähig ist, wenn keine Berechtigung für den Zugriff auf das Mikrofon erteilt wurde. Die Benutzbarkeit soll unter jeder Bedingung stabil bleiben und eine der Aufgaben des Testers ist es, genau das sicherzustellen.

Warum Testen Vertrauen fördert

Durch Mobile App Testing wird Vertrauen nicht dem Zufall überlassen, sondern aktiv gesichert. Wenn wir durch eine strategische Geräteauswahl die Fragmentierung des Marktes abdecken, durch Feldtests die Tücken des mobilen Alltags vorwegnehmen und die Sicherheit unserer persönlichsten Daten garantieren, dann machen wir Qualität für den Endnutzer erst spürbar.

Gutes Testen sorgt dafür, dass die App genau der verlässliche Partner bleibt, den wir in unserer Hosentasche erwarten. Am Ende des Tages bedeutet Vertrauen in eine App nämlich genau das: Dass man sie einfach benutzen kann, ohne darüber nachdenken zu müssen, ob sie funktioniert – weil die Qualitätssicherung genau das bereits sichergestellt hat.

Abbildung 2: Quelle: Bild generiert von Gemini (Google AI)

Quellen und weiterführende Informationen:

Basiswissen Mobile App Testing. Björn Lemke & Nils Röttger; dpunktverlag (1. Auflage, 2021)

Tanja Huber ist Consultant bei SEQIS.

Zusätzlich zu ihrer Erfahrung in den Bereichen Testfallerstellung, Testdurchführung und Testunterstützung ist sie auch in den Bereichen Projekt- und Qualitätsmanagement tätig.

Beim Herangehen an neue Aufgaben ist ihr eine gewissenhafte Vorgehensweise und kreative Aufgabenlösung wichtig. Ebenso legt sie größten Wert auf hochwertige Qualitätssicherung.

Qualitätssicherung „as a Service“: Warum externe Expertise die Objektivität und damit das Vertrauen stärkt

von Eric Pieber

Unsere globale digitale Infrastruktur gleicht heute einem verteilten, hochgradig interdependenten System. Die Integration von Cloud-Architekturen, Microservices und KI treibt die Innovationsgeschwindigkeit auf die Spitze – verschärft aber gleichzeitig die Anfälligkeit der Systeme drastisch. Wenn fundamentale Systemausfälle eintreten, offenbaren sich die enormen wirtschaftlichen und gesellschaftlichen Risiken einer betriebsblinden Qualitätssicherung.

Softwarequalität ist längst kein nachgelagerter Kontrollschritt mehr. Sie ist eine strategische, proaktive und absolut objektive Notwendigkeit für das Überleben und den Ruf eines modernen Unternehmens. Die ökonomische Notwendigkeit ist seit Jahrzehnten belegt. Fehler, die erst in der Produktion entdeckt werden, verursachen bis zu 100-mal höhere Kosten als solche, die bereits in der Architektur- oder Designphase identifiziert werden [1]. In diesem risikobehafteten Umfeld etabliert sich „Quality Assurance as a Service“ (QAaaS) als disruptives Paradigma. Es bietet neben Skalierbarkeit vor allem einen unschätzbaren psychologischen Vorteil: absolute Unabhängigkeit.

Die Psychologie der Softwareentwicklung und der „Developer Bias“

Die Notwendigkeit einer unabhängigen Qualitätssicherung resultiert nicht aus einem Mangel an technischen Fähigkeiten der internen Teams, sondern aus den unveränderlichen Konstanten der menschlichen Psychologie. Kognitive Verzerrungen wie der Confirmation Bias (Bestätigungsfehler) sind tief in der menschlichen Informationsverarbeitung verwurzelt [2]. Sie führen unweigerlich dazu, dass interne Entwickler – meist völlig unbewusst – Tests entwerfen, die vor allem den „Happy Path“ validieren und Gegenbeweise für die Funktionalität ihres eigenen Codes systematisch ausblenden [3].

In meiner Praxis zeigt sich immer wieder, Qualitätssicherung ist ebenso sehr eine kulturelle wie eine technische Herausforderung. In einem großangelegten Kernbankenprojekt stießen wir anfangs auf Skepsis; die gezielte externe Überprüfung von Komponenten wurde oft als „Überwachungsinstrument“ missverstanden. Dieser Knoten ließ sich nicht durch starre Management-Direktiven lösen, sondern nur durch den persönlichen Dialog auf allen Ebenen.

In Einzelgesprächen, vom Abteilungsleiter bis hin zum neuesten Entwickler, konnte ich darlegen, dass wir alle am gleichen Ziel arbeiten: der Systemstabilität. Die Betonung lag dabei darauf, gemeinsam an einem Strang zu ziehen und kein „Finger Pointing“ zu betreiben. Es geht nicht darum, Schuldige zu finden, sondern stets die Qualität zu gewährleisten. Durch diese transparente Kommunikation und die Positionierung als objektiver Externer, der frei von internem Hierarchiedruck agiert, wandelte sich die anfängliche Abwehrreaktion in exzellente Kooperation und tiefes gegenseitiges Vertrauen. Das Ergebnis war ein reibungsloser Informationsfluss und eine maßgeblich gesunkene Ausfallrate.

Skalierbarkeit und der strategische Wert von QAaaS

Der strategische Wert von QAaaS wird heute in der Führungsetage über Risikominimierung und Innovationsgeschwindigkeit definiert. Die schiere Menge an komplexen Cloud-Migrationen macht rein internes Testing zunehmend zum Flaschenhals. QAaaS erlaubt ein dynamisches Skalieren der Testkapazitäten, ohne unrentable Fixkosten für den permanenten Aufbau von Infrastruktur zu erzeugen. Externe Experten bringen sofort nutzbares, produktives Automatisierungs-Know-how mit, während sich interne Entwickler ungestört auf ihre Kernkompetenz konzentrieren können: Die Wertschöpfung für das Business.

Funktionale Tests - Die Synergie aus Automatisierung und strukturierter Exploration

Im funktionalen Testing zeigt sich wahre Expertise in der strategischen Balancierung verschiedenster Methoden. Interne Teams reduzieren sich unter Zeitdruck oft auf ein rigides „Malen nach Zahlen“ mit streng geskripteten Tests. Automatisierung ist exzellent für Regressionen, doch Skripte finden nur die Fehler, nach denen sie explizit suchen.

Hier greift die methodische Stärke des Exploratory Testing. Im Management existiert oft das Vorurteil, manuelles Testen sei planloses „Herumprobieren“. Die professionelle Realität sieht anders aus. Hochwertiges exploratives Testen ist Session-Based (strikt vorgegebene Zeitlimits) und folgt klaren methodischen Leitplanken [4]. Jede Session deckt nicht nur Lücken auf, die Skripte noch nicht integriert haben, sondern liefert ein tiefes Gefühl für die Stärken und Schwächen des Systems – Erkenntnisse, die direkt in die Risikobewertung und zukünftige Testautomatisierungspläne fließen.

Der menschliche Faktor und Domänenwissen

Menschliche Interaktionen lassen sich algorithmisch nur schwer vollständig antizipieren. Ein End-

nutzer, der im 10-Finger-System rasant tippt, die Tab-Taste einen Sekundenbruchteil zu früh erwischt und ein unbemerktes Leerzeichen hinterlässt, bringt oft ganze Datenverarbeitungsketten zum Einsturz. Ein weiteres Beispiel: Das schnelle Wechseln zwischen einem externen Drittsystem und dem Hauptprozess über den „Zurück“-Button provoziert oft Zustandsfehler in der Session, die kein starrer Testfall abdeckt.

Der größte Hebel entsteht hierbei in kollaborativen Sessions. Ein erfahrener interner Experte liefert das Systemwissen, während der Externe die Objektivität des echten Endnutzers einbringt. Gepaart mit Domänenwissen – etwa bei komplexen Banking-Prozessen – entfällt die mühsame Verifizierung des Grundzustands; man fokussiert sich direkt auf die bekannten, fehleranfälligen Zwischenschritte.

End-to-End (E2E) Testing - Validierung der ganzheitlichen Nutzerreise

E2E-Testing ist weit mehr als eine technische Notwendigkeit; es ist die Lebensversicherung für den digitalen Erfolg. Ein System mag auf der Ebene der Microservices perfekt orchestriert sein und technisch fehlerfrei skalieren – doch wenn unter realer Produktionslast der finale Bestätigungs-Button im Frontend auch nur für wenige Sekunden einfriert oder ein angebundener Drittdienst in ein Timeout läuft, bricht die gesamte Prozesskette abrupt ab. Externe Experten betrachten E2E-Tests daher nicht isoliert als rein technische Disziplin, sondern als genau die Schnittstelle, an der Technologie und Business nahtlos verschmelzen. Es geht hierbei um den unbestechlichen Nachweis, dass der gesamte Geschäftsprozess aus der Perspektive des Endkunden durchgängig funktioniert.

Ein klassischer und in der Praxis oft fataler Irrweg vieler interner Teams ist der Versuch, absolut jedes erdenkliche funktionale Szenario über die Benutzeroberfläche (UI) abzufangen – ein Phänomen, das auch als „Ice-Cream Cone Anti-Pattern“ bekannt ist. Dieser Ansatz führt, wie empirisch belegt ist, zwangsläufig zu extrem hohen Wartungsaufwänden und instabilen „Flaky Tests“[5]. Minimale Latenzen beim Rendern des DOMs, winzige Design-Anpassungen im CSS oder asynchrone Netzwerkverzögerungen lassen diese Tests immer wieder fehlschlagen. Das zerstört das Vertrauen in die Automatisierung, blockiert Release-Zyklen massiv und und erhöht die Wartungsaufwände für die Testautomation enorm.

In meiner Consulting-Praxis setze ich daher konsequent auf eine strategische Entflechtung der Testebenen. Die ressourcenintensive Last wird hocheffizient und isoliert auf der API-Ebene generiert. Zeitgleich durchlaufen gezielte, stark fokussierte E2E-Tests (beispielsweise via Playwright) ausschließlich die kritischsten, relevantesten Nutzerpfade in der UI. Durch diese parallele Ausführung messen wir sofort und realitätsnah, wie sich die Backend-Last auf die spürbare Latenz beim Endnutzer auswirkt, ohne die Testinfrastruktur selbst zum Flaschenhals zu machen. Moderne, KI-gestützte Suiten – etwa durch „Self-Healing“-Mechanismen bei dynamischen UI-Elementen – ermöglichen es uns heute zudem, dass diese robusten Smoke-Tests in wenigen Minuten direkt in der CI/CD-Pipeline laufen und fehlerhafte Releases zuverlässig blockieren, noch bevor sie echten geschäftlichen Schaden anrichten.

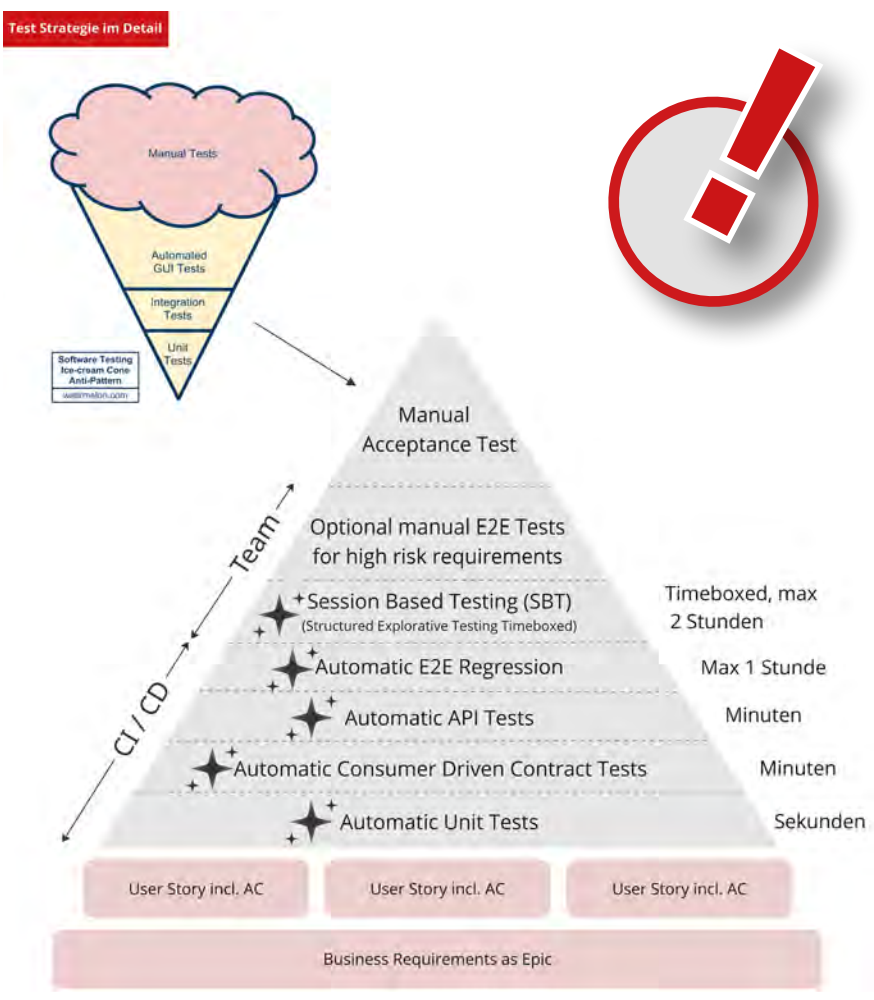


Abbildung 1: Testing Pyramide im Vergleich zum “Ice-Cream-Cone” Anti-Pattern
Quelle: SEQIS Group GmbH

Abbildung 2: Quelle: Bild generiert von Gemini (Google AI)

Performance Engineering - Proaktive Architekturbewertung statt reaktiver Brandbekämpfung

Ein proaktives Performance Engineering stützt die Architektur bereits in der Konzeptphase, anstatt Engpässe erst kurz vor dem Go-Live panisch zu flicken.

In einem großangelegten Kernbankenprojekt etablierten wir einen standardisierten Prozess.
Jedes Deployment musste zwingend eine dedizierte Performance-Umgebung passieren. Da eine 1:1-Simulation der Produktionslast oft illusorisch ist, nutzten wir dort teil-erhöhte Lasten, um grobe Architekturschnitzer frühzeitig zu filtern. Die finale Validierung fand pragmatisch nachts direkt in der Produktion statt – zu Zeiten minimaler Nutzeraktivität, wodurch das wirtschaftliche Risiko gegen Null ging. Denn grobe Fehler entdeckt man bereits mit erhöhter Last in der Performance-Umgebung, und das verbleibende Restrisiko wird in der Produktion bei geringem User-Aufkommen validiert.

Entscheidend war auch hier der persönliche Dialog. Abteilungen, die das gezielte Stressten ihrer APIs als Chance begriffen, produzierten in der Folge nahezu keine Ausfälle. Andere Teams reagierten anfangs defensiv, da sie externe QA als Überwachungsinstrument missverstanden. Erst durch die Kommunikation von Mensch zu Mensch – vom Manager bis zum neuesten Developer – konnte ich darlegen, dass ich als objektiver Externer keinen internen Druck weitergebe, sondern nur die Stabilität erhöhen will. Diese Transparenz führte dazu, dass Teams die Belastungstests schließlich selbst forderten, was die Ausfallrate im System maßgeblich senkte.

Im Folgenden illustriere ich ein weiteres Beispiel illustrieren, welches den Wert methodischer Tiefe aufzeigt.
Bei einem Enterprise-Kunden herrschte Unklarheit über das Cloud-Sizing für ein massives Kunden-Onboarding. Erst unsere Einführung detaillierter Einzelreports und systematischer Vergleichsanalysen offenbarte schonungslos, dass die internen Erwartungen an das System programmatisch gar nicht realisierbar waren. Wir lieferten die Datengrundlage für gezielte Refactorings, anstatt blind in einen Produktionsausfall zu laufen. Wir messen dabei nicht nach Durchschnittswerten. Sondern nach unbestechlichen Perzentilen (p95, p99), da Averages die kritische Wahrheit über Systeminstabilitäten oft verschleiern,weiters werden immer für die zu beantwortenden Fragen relevante Metriken herangezogen, um möglichst präzise Aussagen treffen zu können.

Unabhängige Verifizierung (IV&V) als Währung des Vertrauens

In hochgradig sicherheitskritischen Sektoren wie der Luft- und Raumfahrt oder der Medizintechnik ist die „Independent Verification and Validation“ (IV&V) seit Jahrzehnten der etablierte Goldstandard [6].

Auch wenn wir uns in typischen Enterprise-Projekten nicht in diesen extrem regulierten Sphären bewegen, ist die Kernphilosophie der IV&V von unschätzbarem Wert. Die konsequente organisatorische und finanzielle Unabhängigkeit des Testteams vom Entwicklungsteam. Wir adaptieren diesen Grundgedanken für die Unternehmensrealität. Anstatt bürokratische Prüfprozesse zu erzwingen, etablieren wir agile Qualitätspartnerschaften auf Basis des DevOps-Paradigma (cross-funktionale, autonome Produktteams).

Wahres Vertrauen entsteht dabei durch absolute Transparenz. Indem wir beispielsweise einheitliche Qualitäts- und Performance-Dashboards etablieren, auf die alle Stakeholder gleichermaßen Zugriff haben, entkoppeln wir die Systembewertung von persönlichem Empfinden. Diese können herangezogen werden, um Vergleiche mit vordefinierten “Quality Gates” zu evaluieren.

Diese eindeutige, messbare und unmissverständliche Objektivität beendet emotionale Debatten zwischen Entwicklern und Management und stellt Investitionsentscheidungen auf ein faktenbasiertes Fundament – sie wird zur echten Währung des Vertrauens (Trust Currency).

Objektivität als kompromissloses Fundament digitaler Exzellenz

QAaaS ist keine simple Kostensenkungsmaßnahme – es ist ein strategischer Imperativ. Genau diese Brücke zwischen der methodischen Strenge echter Unabhängigkeit und der partnerschaftlichen Flexibilität zu schlagen, ist der Kern unserer Philosophie bei SEQIS.

Erfahrene QA-Spezialisten transformieren die Qualitätssicherung von einem lästigen Kontrollschritt zu einer wertschöpfenden Instanz, die Teams befähigt und Führungskräften Sicherheit gibt. Wer heute in externe Objektivität investiert, investiert in die Resilienz, in tiefe partnerschaftliche Zusammenarbeit und in die zukunftssichere Skalierbarkeit seines gesamten digitalen Ökosystems.

Abbildung 3: Quelle: Bild generiert von Gemini (Google AI)

Quellen:

[1] B. W. Boehm, Software Engineering Economics. Prentice-Hall, 1981
[2] R. S. Nickerson, „Confirmation bias: A ubiquitous phenomenon in many guises,“ Review of General Psychology, vol. 2, no. 2, pp. 175–220, 1998
[3] G. Calikli and A. Bener, „Influence of confirmation bias on software quality,“ Software Quality Journal, vol. 21, no. 2, pp. 159–190, 2013
[4] J. Bach, „Exploratory Testing Explained,“ Satisfice Inc., v.1.4, 2003
[5] Q. Luo, f. Hariri, L. Eloussi, and D. Marinov, „An exploratory study of flaky tests,“ Proc. 22nd ACM SIGSOFT Int. Symp. Foundations of Software Engineering, 2014, pp. 102–113
[6] IEEE, „IEEE Standard for System, Software, and Hardware Verification and Validation,“ IEEE Std 1012-2016, 2017

Eric Pieber ist Senior Consultant.

Durch sein Studium der Wirtschaftsinformatik und Big Data Systems, ist er in der Lage sich mit diversesten Systemarchitekturen auseinander zu setzen. Auch die Rolle des Vermittlers zwischen Fachbereichen und der Entwicklung ist im nichts neues.

In seiner bisherigen Laufbahn hat er sich insbesondere mit den Themen der Prozessoptimierung, Entwicklung, Requirements Engineering, AI, Business Blockchain Anwendungen, sowie auch dem Performance Engineering und Last- und Performance Tests auseinandergesetzt.

Vom Bug-Reporting zum Quality Consulting: Warum Beratung der nächste Schritt nach dem Finden von Fehlern ist

von Fatemeh Ghaffaari

Die fundamentale Transformation der Paradigmen im modernen Software-Engineering hat die Rolle von Testexperten grundlegend gewandelt. Diese Entwicklung vollzieht sich weg von rein exekutiven Operatoren hin zu strategischen Beratern, die tief in die Geschäfts- und Entwicklungsprozesse einer Organisation integriert sind. In einer Ära, in der eine extrem kurze Markteinführungszeit (Time-to-Market) bei gleichzeitig kompromissloser Qualität gefordert wird, erweisen sich traditionelle Ansätze als zunehmend unzureichend. Das herkömmliche Modell, welches das Testen als isolierte Phase am Ende des Entwicklungszyklus betrachtete, kann den heutigen geschäftlichen Anforderungen nicht mehr gerecht werden. Ein einfacher Fehlerbericht ist zwar weiterhin ein notwendiger Bestandteil der operativen Tätigkeit, reicht jedoch als alleiniges Instrument bei weitem nicht mehr aus, um die immensen Kosten zu verhindern, die durch Softwaredefekte entstehen.

Abbildung 1: Quelle: Bild generiert von Gemini (Google AI)

Industriestatistiken belegen eindrucksvoll die wirtschaftliche Notwendigkeit dieses Wandels. Die Kosten für die Behebung eines Fehlers in der Produktionsphase können schnell bis zu hundertmal höher sein als die Identifizierung desselben Mangels während der frühen Anforderungs- oder Designphase. Diese Analyse untersucht den Übergang vom reinen Finden von Fehlern hin zur Cross-functional Quality Engineering bzw. Full-Lifecycle QA-Strategy und erläutert, warum die beratende Funktion die notwendige evolutionäre Stufe nach der Beherrschung technischer Testfertigkeiten darstellt.

Theoretische Fundamente der Transformation: Abgrenzung der Qualitätsdisziplinen

Um die Tiefe des Konzepts der Qualitätsberatung zu erfassen, ist eine präzise terminologische Abgrenzung der oft synonym verwendeten Begriffe Softwaretesten, Qualitätssicherung (QA) und Quality Engineering (QE) bzw. Qualitätsberatung erforderlich. Softwaretesten ist traditionell eine reaktive Tätigkeit, die darauf fokussiert ist, Abweichungen zwischen dem Ist- und Soll-Zustand eines fertigen Produkts zu identifizieren. Die Qualitätssicherung (QA) hingegen ist prozessorientiert und proaktiv gestaltet. Ihr Ziel ist es, sicherzustellen, dass die angewandten Prozesse tatsächlich zu einem qualitativ hochwertigen Endprodukt führen ("Der Weg ist das Ziel").

Die Qualitätsberatung oder das Quality Engineering (QE) geht über diese Definitionen hinaus. Hier wird Qualität als integrale Kultur und gemeinsame Verantwortung innerhalb der gesamten Organisationsstruktur verankert. Der Qualitätsberater fungiert nicht als Gatekeeper, sondern als Wegbereiter, der Systeme so konzipiert, dass sie inhärent stabil sind.

Die folgende Tabelle verdeutlicht die strukturellen Unterschiede zwischen den verschiedenen Reifegraden der Qualitätssicherung:

Abbildung 2: Quelle: Bild generiert von Gemini (Google AI)

Die Analyse dieser Daten verdeutlicht, dass ein Qualitätsberater nicht mehr nur die Frage beantwortet, ob ein Produkt funktioniert. Vielmehr steht die strategische Fragestellung im Vordergrund, wie die Organisation befähigt werden kann, Produkte zu entwickeln, die von Beginn an frei von strukturellen Mängeln sind. Dies erfordert ein tiefes Verständnis von Lean-Prinzipien und agilen Werten.

Ökonomische Dimensionen und das Management verborgener Kosten

Die Notwendigkeit des Übergangs zur Beratung ist untrennbar mit der ökonomischen Steuerung von Softwareprojekten verknüpft. Die Qualitätskosten setzen sich aus Präventionskosten, Prüfkosten sowie internen und externen Fehlerkosten zusammen. Testanalysten in beratender Funktion unterstützen Organisationen dabei, die Anhäufung technischer Schulden zu vermeiden, indem sie eine konsequente „Shift-Left"-Strategie implementieren.

Abbildung 3: Quelle: Bild generiert von Gemini (Google AI)

Ein Qualitätsberater schafft Mehrwert, indem er präventive Methoden etabliert, die nachweislich die Gesamttestkosten um bis zu 50 Prozent senken und die Time-to-Market erheblich beschleunigen können. Dieser strategische Beitrag übersteigt die rein operative Fähigkeit eines Testers, lediglich oberflächliche Fehler zu finden. Die Implementierung von Continuous Compliance und automatisierten Teststufenkonzepten ist hierbei ein zentraler Erfolgsfaktor.

Ein zentrales Instrument des Beraters ist der risikobasierte Testansatz. Hierbei berät der Experte die Stakeholder darüber, welche Systembereiche die höchste Ausfallwahrscheinlichkeit und die gravierendsten geschäftlichen Auswirkungen haben. Dies ermöglicht eine optimale Priorisierung begrenzter Testressourcen.

Modern Testing Principles: Die Roadmap für Qualitätsberater

Im Jahr 2017 definierten Alan Page und Brent Jensen die „Modern Testing Principles", die den beratenden Charakter der Testrolle im Zeitalter von DevOps und Agilität unterstreichen. Diese Prinzipien fordern eine Abkehr von der Rolle des Testers als „Sicherheitsnetz". Stattdessen hat das das gesamte Team "Shared Responsibility" und „Quality Ownership". Die Kernprinzipien umfassen unter anderem:

- Geschäftsorientierung: Das Ziel ist die Verbesserung des Business, nicht nur das Finden von Fehlern.
- Beschleunigung: Nutzung von Lean-Thinking zur Eliminierung von Prozessengpässen.
- Kultur vor Kontrolle: Förderung einer Kultur der Qualität anstelle von starren Kontrollmechanismen.
- Datengetriebene Entscheidungen: Einsatz von Feedbackschleifen zur Validierung von Produkthypothesen.

Dieser Paradigmenwechsel vom „Testen durchführen" zum „Qualität ermöglichen" bildet den Kern der modernen Qualitätsberatung. Die Rolle entwickelt sich hin zum Generalist oder „Generalizing Specialist", dessen Stärke in der Breite des Wissens liegt.

Transition zur Rolle des Quality Coach in agilen Umgebungen

In agilen Teams wandelt sich die Rolle des Testers zunehmend zum „Quality Coach". Ein Quality Coach schreibt nicht mehr notwendigerweise alle Testfälle selbst, sondern koordiniert die Aktivitäten zwischen Entwicklung und Test. Er fungiert als Mentor, der dem Team beibringt, wie man qualitativ hochwertige Software baut.

Aufgaben eines Quality Coach im skalierten Umfeld (SAFe)

Im Scaled Agile Framework (SAFe) wird die Rolle des Quality Coach auf verschiedenen Ebenen (Team, Programm, Large Solution, Portfolio) eingeführt. Seine Ziele sind:

- Förderung der Zusammenarbeit: Durchführung von Workshops und gemeinsamen Tests zur Schaffung eines gemeinsamen Verständnisses der Anforderungen.
- Wissenstransfer: Coaching der Mitarbeiter in agilen Praktiken wie Test-Driven Development (TDD) und Pair Programming.
- Strategische Ausrichtung: Sicherstellung, dass die richtigen QS-Maßnahmen zur richtigen Zeit eingesetzt werden und der Qualitätsgedanke jederzeit präsent ist.

Ein Quality Coach trägt dazu bei, dass Qualität nicht als Hindernis, sondern als Beschleuniger für Business Agility wahrgenommen wird. Er hilft dabei, Missverständnisse zu vermeiden und die Effizienz innerhalb des Projekts zu steigern. Der Erfolg wird nicht mehr an der Anzahl der gefundenen Bugs gemessen, sondern an der Stabilität des Systems und der Zufriedenheit der Kunden.

Moderne Werkzeuge und Technologien im Dienst der Beratung

Ein Qualitätsberater muss über umfassende Kenntnisse der Werkzeuglandschaft verfügen, um Organisationen fundiert beraten zu können. Dies umfasst nicht nur traditionelle Testautomatisierungstools, sondern auch moderne CI/CD-Pipelines und KI-gestützte Lösungen.

Ein Berater muss Organisationen dabei unterstützen, Generative KI verantwortungsvoll im Test-Lebenszyklus einzusetzen. Dies umfasst Aspekte wie Prompt Engineering, Risikomanagement und den Aufbau einer LLM-gestützten Testinfrastruktur, wobei bei letzteren auf die Risiken wie Halluzinationsrisiken und Data Privacy besonders hinzuweisen ist. KI kann bei der Generierung von Testfällen und der Analyse großer Datenmengen unterstützen, erfordert jedoch eine kritische Bewertung der Ergebnisse.

Professionelle Testautomatisierung

wird heute als eine Entwicklungsaufgabe verstanden. Der Berater hilft bei der Auswahl zwischen verschiedenen Frameworks (z.B. für Mobile Applications oder Web-Services) und sorgt dafür, dass die Testumgebungen dynamisch und wartbar bleiben.

Methodik zur Implementierung von Qualitätsberatung in Organisationen

Für Unternehmen wie SEQIS ist eine systematische Herangehensweise entscheidend. Ein Standardprozess der Beratung umfasst typischerweise folgende Phasen:

- Assessment: Auditierung des aktuellen Testreifegrades unter Verwendung von Modellen.
- Strategieentwicklung: Entwurf eines maßgeschneiderten Testprozesses, der sowohl klassische als auch agile Projekte unterstützt.
- Befähigung: Durchführung von Trainings und Workshops für Tester und Entwickler.
- Kontinuierliche Optimierung: Regelmäßige Überprüfung der Testeffektivität und Anpassung der Strategie an neue technologische Herausforderungen.

In der Praxis zeigt sich, dass der Erfolg einer solchen Transformation stark von der kulturellen Akzeptanz im Unternehmen abhängt.

Fazit: Beratung als finale Mission des Testexperten

Der Übergang vom Fehler-Berichterstatter zur Qualitätsberatung ist eine tiefgreifende Weiterentwicklung der professionellen Identität. Das Identifizieren von Defekten bleibt eine wertvolle technische Basis, doch erst die Fähigkeit, diese Erkenntnisse in strategische Vorteile für das Unternehmen zu verwandeln, definiert den modernen Qualitätsberater. Durch den Fokus auf Prävention statt Korrektur, Coaching statt Kontrolle und Risikomanagement statt blinder Testabdeckung wird der Berater zum Architekten des Vertrauens in einer zunehmend komplexen digitalen Welt. Die Zukunft der Softwarequalität liegt in den Händen derer, die in der Lage sind, Qualität als ersten Baustein jedes Produkts in den Köpfen aller Beteiligten zu verankern. Dies ist der einzige Weg, um in einem hochdynamischen Marktumfeld nachhaltig erfolgreich zu sein.

Abbildung 4: Quelle: Bild generiert von Gemini (Google AI)

Fatemeh Ghaffaari ist Consultant bei SEQIS.

Mit über einem Jahrzehnt Erfahrung in der Qualitätssicherung, insbesondere im Bank- und IT-Dienstleistungsbereich, bringt sie beeindruckende Expertise mit. Ihre Leidenschaft gilt der Sicherstellung der Qualität von Webanwendungen und APIs, wo sie täglich komplexe Herausforderungen meistert. Mit einem Masterabschluss in Physik und einer Spezialisierung auf Testplanung, -analyse, funktionale Tests und Defect-Management zeichnet sie sich durch analytisches Denken und die Fähigkeit aus, innovative Lösungen im Team einzubringen.

Quellen:

Page, A., & Jensen, B. Modern Testing Principles Postulates. Ministry of Testing. https://www.ministryoftesting.com/insights/the-modern-testing-principles

Biffl, S., et al. (2022). Software Quality: The Next Big Thing. Software Quality Days (SWQD), Vienna. Springer. DOI: 10.1007/978-3-031-04115-0_9 https://repositum.tuwien.at/handle/20.500.12708/152207

Buono, P., et al. (2025). Bug Detective and Quality Coach: Developers' Mental Models of AI-Assisted IDE Tools. arXiv preprint. https://arxiv.org/abs/2511.21197

Luo, X., et al. (2025). Whole-Process Consulting Service Quality (WPCSQ) - Model TEOK. Buildings, MDPI. https://www.mdpi.com/2075-5309/15/2/255

Milošević, D. (2022). Perspectives on Quality and Quality Assurance in the Management Consulting Sector (ISO 20700). https://www.researchgate.net/publication/361278042_Perspectives_on_Quality_and_Quality_Assurance_in_the_Management_Consulting_Sector

Baggen, R., et al. (2011). Standardized Code Quality Benchmarking for Improving Maintainability (Based on ISO/IEC 9126). https://www.researchgate.net/publication/227074069_Standardized_code_quality_benchmarking_for_improving_software_maintainability

Wagner, S. (2010). Ein Kosten-Nutzen-Modell für die Softwareprüfung. Universität Stuttgart. https://www2.informatik.uni-stuttgart.de/bibliothek/ftp/ncstrl.ustuttgart_fi/DIS-2010-05/DIS-2010-05.pdf

Zhu, J., et al. (2024). AI-Driven Transformation in Quality Engineering: From Legacy Practices to Continuous Multi-Vendor Testing.

Seidl, R. Software Tester Evolution: From Bug Hunter to Quality Consultant. https://www.richard-seidl.com/en/podcast/software-tester-evolution/

Seidl, R. SAFe und Qualität: Strategien für agile Skalierung. https://www.richard-seidl.com/de/podcast/safe-qualitaet/

Tea-time with Testers (2021). Quality Engineering Edition. July Issue. https://teatimewithtesters.com/wp-content/uploads/2021/07/TTwT_July_2021-1.pdf

Ministry of Testing Community. Discussions on Quality Engineering & Changing Responsibilities. [Forum Threads]. Available at:
https://club.ministryoftesting.com/t/can-we-talk-about-quality-engineering/64554
https://club.ministryoftesting.com/t/what-s-one-way-you-ve-seen-responsibilities-for-quality-change/86762

Europas Dritter Weg: Die EU-Architektur für eine sichere und faire Digitalisierung

von Alexander Lewisch

Der Regulierungsrahmen der EU zur Digitalisierungsstrategie

Einleitung
Das Internet, einst als grenzenloser Raum der Freiheit und der unbegrenzten Möglichkeiten gefeiert, hat in den letzten zwei Jahrzehnten sein Gesicht gewandelt. Aus der Utopie einer uneingeschränkt globalen Vernetzung ist eine Arena harter geopolitischer Interessen, ökonomischer Monopole und neuer Sicherheitsrisiken geworden. Die Zeit des digitalen "Laissez-faire", in der sich Technologie schneller entwickelte als die Demokratie reagieren konnte, neigt sich dem Ende zu. Nirgendwo auf der Welt wird dieser Paradigmenwechsel so konsequent vollzogen wie in der Europäischen Union.

Was Kritiker oft als bürokratische „Regulierungswut" oder ökonomischer "Bremsklotz" bezeichnen, ist bei genauer Betrachtung der historisch notwendige Versuch, die staatliche und bürgerliche Souveränität im digitalen Raum zurückzugewinnen. Die EU hat erkannt, dass Daten ein fruchtbarer Nährboden sind, auf dem gesellschaftlicher Einfluss, wirtschaftliche Dominanz und nationale Sicherheit gedeihen. Daher schafft Brüssel einen Referenzstandard aus Verordnungen und Richtlinien, der von der Datenschutz-Grundverordnung (DSGVO) bis zur KI-Verordnung (AI Act) reicht, um im globalen Wettbewerb mit den USA und China seine Ziele zu erreichen.

Der Dritte Weg: Digitaler Humanismus zwischen Silicon Valley und Staatskapitalismus
Um die aktuelle Flut an Rechtsakten zu verstehen, muss man den Blick auf die globalen Pole richten. Auf der einen Seite steht das US-amerikanische Modell, geprägt vom „Silicon Valley"-Ethos: Maximale Freiheit für Märkte, „Move fast and break things" und eine Dominanz privater Plattformen, die faktisch die Regeln der öffentlichen Kommunikation diktieren. Auf der anderen Seite steht das Modell des digitalen "Staatskapitalismus" der Kommunistischen Partei Chinas, in dem Technologie primär der sozialen Kontrolle und staatlichen Sicherheitsinteressen dient.

Europa hat sich entschieden, keinem dieser Modelle zu folgen. Die Strategie der EU-Kommission zielt auf einen „Dritten Weg", den des Digitalen Humanismus, ab. Die Grundthese lautet, dass Technologie dem Menschen dienen muss und nicht umgekehrt. In ihrer Agenda für ein Europa, das fit für das digitale Zeitalter ist, definiert die Kommission Regulierungen nicht als Innovationsbremse, sondern als vertrauensbildende Maßnahme. Nur wenn Bürger und Unternehmen darauf vertrauen können, dass ihre Daten sicher sind, Algorithmen nicht diskriminieren und Infrastrukturen nicht ausfallen, werden sie diese Technologien auch verinnerlichen.[1]

Abbildung 1: Quelle: Bild generiert von Gemini (Google AI)

Von der Abwehr zur Gestaltung: Der Wandel der Rechtsarchitektur

Lange Zeit galt die Datenschutz-Grundverordnung (DSGVO) als der einsame Leuchtturm der EU-Digitalpolitik. Sie war ein Schutzschild, konzipiert, um die Privatsphäre des Einzelnen gegen den Datenhunger der Marketingabteilungen und der Werbeindustrie zu verteidigen. Doch die Realität der 2020er Jahre erforderte ein Umdenken. Ein Schutzschild allein reicht nicht, wenn die Infrastruktur selbst angegriffen wird oder wenn wenige Gatekeeper den Marktzugang kontrollieren. Daher hat die EU ihre Strategie erweitert. Es geht nicht mehr nur um Schutz (Protection), sondern um Ordnung (Governance) und Resilienz (Security). Man kann die neuen Gesetze als Bausteine einer einzigen großen Architektur betrachten, die drei fundamentale Defizite des digitalen Marktes korrigieren soll.

Das Sicherheitsdefizit und Schutz der Grundrechte

Die DSGVO bildete das historische Fundament dieser Architektur, indem sie den Schutz der Privatsphäre und die Hoheit über personenbezogene Daten als unumstößliches Grundrecht verankerte. Doch dieses Recht auf informationelle Selbstbestimmung bleibt theoretisch, wenn die IT-Infrastrukturen angreifbar sind. Mit der zunehmenden Vernetzung schutzbedürftiger Infrastrukturen, wie etwa Gesundheitseinrichtungen, Energienetzen und Finanzsystemen, ist Cybersicherheit zu einer Frage der nationalen Sicherheit geworden. Als Reaktion auf bestehende Bedrohungen setzt die EU auf ein Trio konsequenter rechtlicher Sicherheitsmaßnahmen. Die NIS-2-Richtlinie zwingt Betreiber kritischer Infrastrukturen zu professionellem Risikomanagement. Der Cyber Resilience Act (CRA) dreht die Logik um und nimmt erstmals die Hersteller von Hard- und Software in die Pflicht, Sicherheit schon im Design zu verankern. Ergänzt wird dies durch den Digital Operational Resilience Act (DORA), der speziell den Finanzsektor gegen digitale Störfaktoren abhärtet.[2]

Das Wettbewerbsdefizit

Da die digitale Ökonomie zur Bildung von Monopolen tendiert, haben Netzwerkeffekte dazu geführt, dass wenige US-Konzerne de facto als Gatekeeper fungieren. Wer nicht im App-Store gelistet ist oder im Suchranking auftaucht, existiert ökonomisch nicht. Hier greifen der Digital Markets Act (DMA) und der Digital Services Act (DSA) ein. Während der DMA den Wettbewerb durch das Aufbrechen von Monopolstrukturen wiederbeleben soll, verpflichtet der DSA die Plattformen zur Übernahme gesellschaftlicher Verantwortung, wie etwa im Kampf gegen Desinformation und Hassrede.[3] Es ist der Versuch, das Grundgesetz auch im digitalen Raum durchzusetzen: „Denn was offline illegal ist, muss auch online illegal sein".[4]

Das Innovationsdefizit

Europa hat den ersten Lauf der Digitalisierung (Consumer Internet, Social Media) weitgehend an die USA verloren. Im zweiten Lauf, dem industriellen Internet der Dinge (IoT) und der Künstlichen Intelligenz, will Europa die Führung übernehmen. Daher sollen der Data Act und der Data Governance Act (DGA) die Silos aufbrechen, in denen Maschinendaten heute oft gefangen sind, um einen fairen europäischen Binnenmarkt für Daten zu schaffen. Gleichzeitig setzt der AI Act weltweit den ersten rechtlichen Rahmen für Künstliche Intelligenz, um Innovation zu ermöglichen, ohne aber ethische Grundsätze zu opfern.[5]

Das „Fundament" der europäischen Digitalregulierung

Die fortschreitende Digitalisierung erfordert eine verlässliche und robuste rechtliche Basis, auf der Unternehmen ihre innovativen Geschäftsmodelle und Datennutzungskonzepte sicher aufbauen können. Dieses „Fundament" des europäischen Compliance-Architektur besteht aus vier zentralen rechtlichen Regelwerken (DSGVO, NIS-2, CRA und DORA), die gemeinsam den essentiellen Basisschutz für Daten, IT-Infrastrukturen und digitale Produkte gewährleisten. Nur wenn der Schutz der individuellen Privatsphäre, die organisatorische Abwehrbereitschaft gegen Cyberbedrohungen und die technische Sicherheit der eingesetzten Hard- und Software lückenlos ineinandergreifen, entsteht eine widerstandsfähige und tragfähige Grundlage, um die darauf aufbauenden, komplexeren Regulierungen der europäischen Digitalstrategie erfolgreich zu meistern.[6]

Die DSGVO als Grundstein des Datenschutzes

Die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) bildet das rechtliche Fundament für den Schutz personenbezogener Daten innerhalb der Europäischen Union. Ihr Hauptziel ist die Wahrung der Grundrechte und der Privatsphäre natürlicher Personen bei der Datenverarbeitung. Zentrale Prinzipien wie Datenminimierung, Zweckbindung und Transparenz sind in Artikel 5 verankert. Zudem verpflichtet Artikel 32 alle verarbeitenden Unternehmen dazu, durch angemessene technische und organisatorische Maßnahmen ein hohes Sicherheitsniveau bei der Verarbeitung dieser Daten zu gewährleisten. Die Datenschutz-Grundverordnung trat formell bereits am 24. Mai 2016 in Kraft. Um den Unternehmen, Behörden und Organisationen ausreichend Zeit für die teilweise massiven rechtlichen und technischen Umstellungen zu geben, wurde eine zweijährige Übergangsphase gewährt. Seit dem Stichtag am 25. Mai 2018 ist das Gesetz in der gesamten Europäischen Union unmittelbar, vollumfänglich und rechtlich bindend anwendbar.[7]

NIS-2 und die Resilienz von Organisationen

Mit der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) weitet die EU den Fokus auf die allgemeine Netz- und

Informationssicherheit von kritischen und wichtigen Einrichtungen aus. Die Regelung verpflichtet Organisationen in Artikel 21 zu einem professionellen und umfassenden Risikomanagement im Bereich der Cybersicherheit, wofür die Geschäftsleitung nach Artikel 20 explizit die Verantwortung trägt. Flankiert werden diese Präventivmaßnahmen durch strenge Meldepflichten gemäß Artikel 23, die vorschreiben, dass erhebliche Sicherheitsvorfälle innerhalb sehr enger Fristen an die zuständigen nationalen Behörden gemeldet werden müssen. Da es sich bei NIS-2 um eine EU-Richtlinie handelt, wirkt sie nicht direkt, sondern muss in nationale Gesetze gegossen werden. Sie trat auf EU-Ebene am 16. Januar 2023 in Kraft. Die nationalen Gesetzgeber der Mitgliedstaaten hatten anschließend, gemäß Artikel 41, eine verbindliche Umsetzungsfrist bis zum 17. Oktober 2024, um die Vorgaben in lokales Recht zu überführen. Ab diesem Datum müssen betroffene Unternehmen die neuen Cybersicherheits- und Meldepflichten in der Praxis erfüllen.[8]

Der Cyber Resilience Act (CRA) für sichere Produkte

Der Cyber Resilience Act (Verordnung (EU) 2024/2847) nimmt erstmals gezielt die Hersteller von Produkten mit digitalen Elementen, also Hard- und Software, in die Pflicht. Der Fokus liegt hierbei auf dem Prinzip der eingebauten Sicherheit („Security by Design"), wodurch wesentliche Sicherheitsanforderungen bereits bei der Entwicklung und Produktion eingehalten werden müssen, was im Anhang I der Verordnung detailliert definiert ist. Zusätzlich verlangt die Verordnung in Artikel 10 und 13, dass Hersteller über den gesamten Lebenszyklus des Produkts, beziehungsweise für einen definierten Zeitraum, Schwachstellen beheben und entsprechende Sicherheitsupdates bereitstellen. Der Cyber Resilience Act wurde Ende 2024 final im EU-Amtsblatt veröffentlicht und trat am 10. Dezember 2024 offiziell in Kraft. Da die Verordnung tiefgreifende Änderungen für die Entwicklung und weltweite Produktion von Hardware und Software erfordert, gewährt der Gesetzgeber eine großzügige Anpassungsphase von 36 Monaten. Die Anforderungen an sichere Produkte müssen demnach erst ab dem 11. Dezember 2027 zwingend erfüllt werden, wobei bestimmte Meldepflichten für Hersteller bezüglich Schwachstellen und Vorfällen bereits vorgezogen werden und ab dem 11. September 2026 (Artikel 71) greifen.[9]

DORA als Spezialgesetz für den Finanzsektor

Der Digital Operational Resilience Act (Verordnung (EU) 2022/2554) ist als strenges Spezialgesetz konzipiert, das ausschließlich die digitale betriebliche Resilienz im europäischen Finanzsektor absichert. Die Verordnung etabliert in den Artikeln 5 bis 16 einen sehr spezifischen und engmaschigen Rahmen für das IKT-Risikomanagement, dem Banken, Versicherungen und andere Finanzdienstleister zwingend folgen müssen. Darüber hinaus regelt DORA in den Artikeln 28 bis 44 detailliert den Umgang mit IKT-Drittparteienrisiken und schreibt in den Artikeln 24 bis 27 regelmäßige, tiefgreifende Tests der operationalen Resilienz, wie beispielsweise szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und bedrohungsgeleitete Penetrationstests, vor. Der Digital Operational Resilience Act trat parallel zur NIS-2-Richtlinie am 16. Januar 2023 in Kraft. Im Gegensatz zu NIS-2 ist DORA jedoch eine Verordnung und gilt somit unmittelbar in allen Mitgliedstaaten, ohne dass es nationale Umsetzungsgesetze braucht. Den Finanzmarktakteuren und ihren IKT-Dienstleistern wurde eine Vorbereitungszeit von genau 24 Monaten eingeräumt. Seit dem 17. Januar 2025 (Artikel 64) sind die strengen regulatorischen Vorgaben für die Branche verbindlich anzuwenden.[10]

Zusammenspiel, Konflikte und Vorrangregeln

Diese vier Gesetzgebungswerke greifen ineinander, um ein ganzheitliches europäisches Schutzniveau zu schaffen. Während der CRA die zugekaufte Technologie an sich sichert, stärkt NIS-2 die Prozesse in der anwendenden Organisation, schützt die DSGVO die in den Systemen verarbeiteten Daten und überwacht DORA den besonders kritischen Finanzmarkt. Bei juristischen Überschneidungen und vorhandenen Mehrfachregulierungen, etwa wenn ein schwerer Cyberangriff auf eine Bank gleichzeitig Meldepflichten für Datenschutz, Systemausfall und IT-Sicherheit auslöst, gilt grundsätzlich das rechtliche Prinzip der Lex specialis (siehe Infobox). Dies bedeutet konkret, dass die sehr spezifischen Anforderungen der DORA-Verordnung für den Finanzsektor den allgemeineren Resilienzvorgaben der NIS-2-Richtlinie gesetzlich vorgehen (siehe Art. 1 Abs. 2 NIS-2).[8, 10]

„Lex specialis derogat legi generali"

Der Grundsatz lex specialis derogat legi generali (lateinisch für „das speziellere Gesetz verdrängt das allgemeinere Gesetz") ist eine fundamentale juristische Kollisionsregel, die in fast allen modernen Rechtsordnungen zur Lösung von Normenkonflikten angewendet wird. Diese methodische Regel greift immer dann, wenn zwei verschiedene Rechtsvorschriften denselben Sachverhalt regeln, sich in ihren Anforderungen oder Rechtsfolgen jedoch überschneiden oder widersprechen. In einer solchen Situation ordnet der Grundsatz an, dass die speziellere Norm – also jene, die den Sachverhalt detaillierter, enger oder für einen besonderen Adressatenkreis regelt – der allgemeiner gefassten Norm zwingend vorgeht.[11]

Europäische Datenökonomie
Auf dem soliden Fundament aus Cybersicherheit und Datenschutz, das IT-Systeme stabilisiert und persönliche Rechte schützt, hat die europäische Gesetzgebung zwei tragende Säulen in ihrer Compliance-Architektur errichtet. Während das Fundament primär einen abwehrenden und sichernden Charakter aufweist, steht bei der ersten Säule, bestehend aus dem Data Governance Act und dem Data Act, die aktive, wertschöpfende und faire Nutzung von Informationen im Vordergrund. Diese Bestimmungen betreffen die europäische Datenökonomie, da sie die rechtlichen Spielregeln dafür definieren, wie Daten aus vernetzten Geräten wirtschaftlich genutzt, über vertrauenswürdige Vermittler freiwillig geteilt und fair zwischen Unternehmen sowie Verbrauchern verteilt werden können, ohne dabei die im Fundament verankerten Sicherheits- und Datenschutzvorgaben zu gefährden.[12]

Der Data Governance Act (DGA) als Vertrauensanker
Der Data Governance Act (Verordnung (EU) 2022/868) schafft den rechtlichen und strukturellen Rahmen zur Förderung des Datenaustauschs und zur Stärkung des Vertrauens in die gemeinsame Datennutzung innerhalb der EU. Der Fokus liegt hierbei nicht auf der Schaffung neuer, zwingender Zugangsrechte, sondern auf der Etablierung sicherer Infrastrukturen für den freiwilligen Datenaustausch. Dies geschieht insbesondere durch die strenge Regulierung neutraler Datenvermittlungsdienste (Data Intermediary) in Artikel 10, die als vertrauenswürdige Mittler zwischen Dateninhabern und Datennutzern agieren sollen, sowie durch die Förderung des sogenannten "Datenaltruismus" für das Gemeinwohl, der in Artikel 16 geregelt ist. Ziel ist es, einen sicheren europäischen Binnenmarkt zu etablieren, in dem öffentliche und private Daten geschützt, aber dennoch innovationsfördernd geteilt werden können.[13]

Der Data Act (DA) zur wirtschaftlichen Datennutzung
Der Data Act (Verordnung (EU) 2023/2854) regelt präzise, wer unter welchen Bedingungen auf generierte Daten zugreifen und diese wirtschaftlich nutzen darf, wobei der Schwerpunkt auf Daten aus vernetzten Geräten (Internet of Things, IoT) liegt. Die Verordnung gewährt Nutzern in den Artikeln 3 und 4 das weitreichende Recht, auf die von ihren Geräten erzeugten Daten zuzugreifen und diese bei Bedarf an Drittanbieter weiterzugeben. Zudem werden in den Artikeln 8 und 9 faire, angemessene und diskriminierungsfreie (FRAND - „Fair, Reasonable, and Non-Discriminatory") Bedingungen für den Datenaustausch zwischen Unternehmen (B2B) festgelegt und in den Artikeln 23 bis 31 strikte Vorgaben gemacht, um den Wechsel zwischen Cloud-Anbietern zu erleichtern und wirtschaftliche Lock-in-Effekte zu verhindern.[14]

Zusammenspiel, Konflikte und Vorrangregeln
In der juristischen und technischen Praxis greifen diese beiden Verordnungen komplementär ineinander. Während der Data Governance Act die vertrauenswürdige Infrastruktur und die Spielregeln für Vermittler bereitstellt (das „Wie" des Datenaustauschs), definiert der Data Act die konkreten wirtschaftlichen Zugangs- und Nutzungsrechte an den Daten selbst (das „Was" und „Wer"). Ein inhaltlicher Konflikt zwischen den beiden Regelwerken besteht kaum, da sie sich in ihrem Anwendungsbereich bewusst ergänzen. Überschneidungen und potenzielle Konflikte gibt es jedoch mit der DSGVO. Hier ordnen sowohl der Data Act als auch der Data Governance Act explizit an, dass beim Fließen von personenbezogenen Daten die DSGVO als absolute Lex specialis Vorrang hat. Der Data Act berechtigt beispielsweise nicht zur Verarbeitung personenbezogener Daten ohne eine Rechtsgrundlage nach Art. 6 DSGVO, wodurch der Datenschutz unangetastet bleibt. Der Vorrang der DSGVO wird auch explizit im DGA im Erwägungsgrund 4 und im DA in Artikel 3 Absatz 5 hervorgehoben.[13, 14]

Sicherer und fairer digitaler Raum
Während die Datenstrategie der EU den sicheren Austausch von Informationen fördert, zielt die zweite große Säule der europäischen Digitalregulierung auf die Infrastruktur des Internets und somit auf die Online-Plattformen selbst ab. Mit dem Gesetz über digitale Dienste (Digital Services Act, DSA) und dem Gesetz über digitale Märkte (Digital Markets Act, DMA) hat die Europäische Union ein umfassendes Regelwerk geschaffen, um das Internet sicherer, transparenter und wettbewerbsfähiger zu machen. Beide Gesetze bilden gewissermaßen das neue digitale Grundgesetz der EU und wirken zusammen als vertrauenswürdiges Bezugselement, die sich aber unterschiedlichen Problemstellungen der Plattformökonomie widmen.

Der Digital Services Act (DSA): Sicherheit und Grundrechte im Netz
Der DSA (Verordnung (EU) 2022/2065) legt den Fokus auf gesellschaftliche Verantwortung und den Schutz der Nutzer. Sein zentraler Leitgedanke lautet: "Was offline illegal ist, muss auch online illegal sein." Er zwingt digitale Dienste, mehr Verantwortung für die Inhalte zu übernehmen, die sie verbreiten. Plattformen müssen ihre Empfehlungsalgorithmen transparent machen (Art. 27) und Nutzern die Möglichkeit geben, diese anzupassen oder abzulehnen. Zudem verbietet der DSA manipulative Designs (Art. 25), sogenannte „Dark Patterns", und zielgerichtete Werbung, die auf sensiblen Daten oder auf Minderjährige abzielt (Art 26 und 28). Hinzu kommen klare und schnelle Meldeverfahren (Notice-and-Action in Art. 16), über die Nutzer illegale Inhalte oder Hassrede melden können. Die

Plattformen sind verpflichtet, auf Meldungen der Nutzer umgehend zu reagieren. Besondere Pflichten gelten für sehr große Online-Plattformen (VLOPs) und Suchmaschinen, die systemische Risiken proaktiv minimieren müssen (Art. 33 bis Art 43).[15]

Der Digital Markets Act (DMA): Fair Play im digitalen Wettbewerb

Während der DSA den Fokus auf Inhalte legt, hat der DMA (Verordnung (EU) 2022/1925) die Marktmacht der Tech-Giganten im Visier. Er richtet sich ausschließlich an sogenannte Gatekeeper, das sind die wenigen riesigen Digitalkonzerne, die eine unumgängliche Schnittstelle zwischen Unternehmen und Verbrauchern bilden. Der DMA soll verhindern, dass diese Konzerne ihre Marktmacht missbrauchen, um den Wettbewerb zu verhindern. Gatekeeper dürfen ihre eigenen Dienste auf ihren Plattformen nicht mehr bevorzugt behandeln (Verbot des Self-Preferencing in Art 6 Abs 5). Ein Suchmaschinenbetreiber darf also beispielsweise den eigenen Preisvergleichsdienst nicht künstlich auf Platz 1 der Suchergebnisse heben. Außerdem bekommen Nutzer mehr Freiheiten. Sie müssen vorinstallierte Apps löschen können (Art 6 Abs 3) und dürfen nicht gezwungen werden, die Bezahlsysteme der Gatekeeper zu nutzen. Zudem schreibt der DMA vor, dass grundlegende Funktionen von Messenger-Diensten, wie z.B. WhatsApp, interoperabel werden müssen, sodass perspektivisch auch Nachrichten über Anbietergrenzen hinweg verschickt werden können (Art 7).[16]

Zusammenspiel, Konflikte und Vorrangregeln

In der Praxis stehen DSA und DMA keineswegs isoliert nebeneinander, sondern greifen oft ineinander, was zu juristischen Reibungspunkten führt. Für die großen Tech-Konzerne, die unter dem DMA als Gatekeeper und unter dem DSA zeitgleich als sehr große Online-Plattformen eingestuft werden, gilt das Prinzip der kumulativen Anwendung, d.h. sie müssen die Pflichten beider Regelwerke parallel erfüllen. Konfliktpotenzial entsteht vor allem dort, wo beide Gesetze denselben Sachverhalt aus unterschiedlichen Blickwinkeln regulieren, wie etwa bei der nutzerbasierten Werbung. Während der DMA die Zusammenführung von Daten aus verschiedenen Plattformdiensten an eine ausdrückliche Nutzereinwilligung knüpft (Art 5), zieht der DSA harte rote Linien, indem personalisierte Werbung auf Basis sensibler Daten (Art 26) oder Werbung an Minderjährige (Art 28) generell verboten sind. Ein „Ja" des Nutzers zu einer Werbemaßnahme nach dem DMA ist noch lange nicht legal gemäß DSA.

Hinsichtlich der Vorrangregeln gilt, dass sich DSA und DMA weder gegenseitig aufheben noch behindern, da sie im Grunde unterschiedliche Schutzziele verfolgen (Nutzersicherheit versus fairer Wettbewerb). Im Vergleich zu anderen Rechtsnormen gibt es jedoch klare Hierarchien. Auch hier bildet die DSGVO die absolute rote Linie, da ihre Regelungen unberührt bleiben und bei der Verarbeitung personenbezogener Daten stets Vorrang haben (siehe Art 2 DMA und Art 1 DMA). Zudem ersetzt der DMA nicht das klassische EU-Kartellrecht (Art 101 und 102 AEUV), sondern ergänzt es präventiv (ex-ante), wie in Art 1 DMA ausdrücklich klargestellt wird.[15, 16, 17]

Das Dach des Compliance-Hauses: Der AI Act

Den Abschluss und das Dach der europäischen Digitalregulierung bildet der AI Act (Details zum AI Act siehe Ausgabe 2 der Quality News des Jahres 2024). Während die bisherigen Gesetzestexte den Zugang zu Daten, deren Verarbeitung sowie die Macht von Plattformen regeln, adressiert der AI Act die darauf aufbauenden intelligenten und automatisierten Entscheidungssysteme. Sein zentraler Vertrauensanker ist ein strikt risikobasierter Ansatz. Die gesetzlichen Anforderungen an ein KI-System steigen proportional zu den potenziellen Gefahren, die es für die Grundrechte, die Gesundheit und die Sicherheit der Bürger birgt. Das Gesetz teilt KI-Systeme im Wesentlichen in verschiedene Risikokategorien ein, an die konkrete Compliance-Pflichten geknüpft sind.

Um fundamentale europäische Werte zu schützen, zieht das Gesetz absolute rote Linien (Unannehmbares Risiko – Verbotene Praktiken (Art. 5). KI-Systeme, die eine unannehmbare Bedrohung darstellen, sind schlichtweg verboten. Dazu gehören beispielsweise „Social Scoring", die unterschwellige kognitive Manipulation von Personen sowie die massenhafte ungerichtete Auslesung von Gesichtsaufnahmen aus dem Internet zum Aufbau von Datenbanken. Den Kern der Compliance (Art 6 und Art 8-22) bilden Systeme mit hohem Risiko, die in sensiblen Bereichen eingesetzt werden, wie etwa in der kritischen Infrastruktur, im Personalwesen, in der Strafverfolgung oder bei der Bonitätsprüfung. Hier greifen die strengsten Compliance-Pflichten vor der Markteinführung. Anbieter müssen ein lückenloses Risikomanagementsystem etablieren (Art. 9), hohe Anforderungen an die Trainingsdaten erfüllen (Art. 10) und eine wirksame menschliche Aufsicht („Human-in-the-loop") garantieren (Art. 14). Bei Systemen mit begrenztem Risiko (Art 50) steht die Transparenz im Vordergrund. Nutzer müssen wissen, dass sie mit einer Maschine interagieren. So gilt etwa für Chatbots, deep fakes oder KI-generierte Texte und Bilder eine klare Kennzeichnungspflicht. Besondere Regeln gelten für KI-Modelle mit allgemeinem Verwendungszweck (Art. 51 ff.). Mit dem rasanten Aufstieg generativer KI wurde das Gesetz um Regeln für sogenannte General-Purpose AI (GPAI) erweitert. Anbieter dieser Basismodelle müssen umfassende technische Dokumentationen erstellen, das Urheberrecht beim Training der Modelle respektie-

ren und bei Modellen mit systemischem Risiko zusätzliche Evaluierungen durchführen.[18]

Zusammenspiel und Vorrangregeln des AI Acts

Der AI Act fügt sich als Dach nahtlos in die europäische Digitalstrategie ein. Der AI Act schafft keine neue Rechtsgrundlage für die Verarbeitung personenbezogener Daten. In Art. 2 Abs. 7 stellt der AI Act explizit klar, dass die Vorgaben der DSGVO unangetastet bleiben und Vorrang haben. Wenn eine Hochrisiko-KI personenbezogene Daten verarbeitet, muss sie also beiden Regelwerken genügen. Ein praktischer Konflikt bzw. Widerspruch besteht beim „Recht auf Vergessenwerden" (= Löschung nach DSGVO) versus dem Bedarf der AI an stabilen, repräsentativen Trainingsdaten. Der AI Act fordert von Hochrisiko-KI ein hohes Maß an Robustheit und Cybersicherheit. Um jedoch bürokratische Doppelprüfungen zu vermeiden, sieht das Gesetz vor, dass Konformitätsbewertungen nach Möglichkeit in bestehende Prüfverfahren der Cybersicherheitsgesetze, wie dem CRA, NIS-2 oder DORA integriert werden sollen.

Eine starke wirtschaftliche Symbiose herrscht auch zwischen dem AI Act und der europäischen Datenstrategie. Während der DGA und der Data Act rechtssicher dafür sorgen, dass Datensilos aufgebrochen und Industriedaten verfügbar gemacht werden, fungiert der AI Act als Qualitätsfilter. Artikel 10 des AI Acts („Daten und Daten-Governance") definiert extrem strenge Anforderungen an die Trainingsdaten von Hochrisiko-KI, um systematischen Bias und Diskriminierung zu verhindern.

Auch beim Thema der Plattformregulierung (DSA/DMA) gibt es wichtige Schnittmengen. Zwingt der DSA große Plattformen, die gesellschaftlichen Auswirkungen der Algorithmen zu überwachen, reguliert der AI Act parallel die technische Beschaffenheit und Zuverlässigkeit der zugrunde liegenden KI-Modelle. Der DMA verbietet Gatekeepern, unlauter Daten ihrer gewerblichen Nutzer abzugreifen, um damit eigene, konkurrierende Dienste zu füttern. Parallel dazu zwingt der AI Act genau diese mächtigen Akteure bei der Entwicklung von Basismodellen (GPAI) zu strengen Dokumentations- und Urheberrechtspflichten (Art. 51 ff.).[18]

Fazit

Mit der schrittweisen Einführung und Verzahnung der ambitionierten Verordnungen und Richtlinien hat die Europäische Union einen historischen Prozess eingeleitet. Ein isolierter Schutzschild wie die DSGVO reicht in der heutigen Ära der vernetzten Infrastrukturen und Plattform-Monopole nicht mehr aus. Stattdessen steht nun eine robuste, in sich geschlossene Compliance-Architektur.

Auf einem stabilen Fundament aus Datenschutz und Cybersicherheit (DSGVO, NIS-2, CRA, DORA) erheben sich die Säulen einer fairen und wertschöpfenden Datenökonomie (DGA, Data Act) sowie einer verantwortungsvollen Plattformökonomie (DSA, DMA). Abgeschlossen wird dieses Konstrukt durch den AI Act, der als Dach die rasanten Entwicklungen der Künstlichen Intelligenz nach strengen, risikobasierten Prinzipien regelt.

Dieser europäische „Dritte Weg" des "digitalen Humanismus" verdeutlicht, dass Regulierung und Innovation keine Gegensätze sein müssen. Vielmehr ist Vertrauen in sichere Daten, unparteiische Algorithmen und faire Märkte die Grundvoraussetzung dafür, dass Gesellschaft und Wirtschaft neue Technologien überhaupt adaptieren. Was Kritiker oft vorschnell als bürokratischen Bremsklotz abtun, ist in Wahrheit der notwendige Versuch, staatliche und bürgerliche Souveränität im digitalen Raum zurückzugewinnen.

Dank des ökonomischen Gewichts des EU-Binnenmarktes entfaltet diese Architektur zudem eine globale Strahlkraft. Ein oft übersehener Aspekt dieser Regelungsdichte ist ihre außenpolitische Wirkung. Die Rechtswissenschaftlerin Anu Bradford prägte dafür den Begriff des „Brussels Effect".[19] Er beschreibt das Phänomen, dass multinationale Konzerne europäische Standards oft weltweit übernehmen, weil es ökonomisch ineffizient wäre, verschiedene technische Standards für verschiedene Märkte zu unterhalten. Die EU versucht damit nicht nur ihren eigenen Binnenmarkt zu regulieren, sondern möchte ihre demokratischen Werte durch Marktmechanismen in den Rest der Welt exportieren. Wenn die Vorgaben der Compliance-Architektur zum internationalen Goldstandard werden, hat die EU nicht nur sich selbst geschützt, sondern die Spielregeln der globalen Digitalisierung aktiv und nachhaltig geprägt.

Weitere spannende Blogartikel finden Sie hier:

www.seqis.com/de/blog-index

Verordnung (VO)/ Richtlinie (RL)	Zentrale Artikel	Kernthema/ Zielsetzung	Inkrafttreten/ Geltungsbeginn
DSGVO VO (EU) 2016/679	**Art. 5** (Grundsätze) **Art. 6** (Rechtmäßigkeit) **Art. 17** (Recht auf Löschung)	Schutz personenbezogener Daten und informationelle Selbstbestimmung	**Inkrafttreten:** 24.05.2016 **Geltungsbeginn:** 25.05.2018
NIS-2 RL (EU) 2022/2555	**Art. 21** (Risikomanagement) **Art. 23** (Meldepflichten)	Hohes Cybersicherheitsniveau für kritische Infrastrukturen und Lieferketten	**Inkrafttreten:** 16.01.2023 **Umsetzung bis:** 17.10.2024
CRA (Cyber Resilience Act) VO (EU) 2024/2847	**Art. 13/14** (Schwachstellen- & Vorfallsmeldung) **Anhang I** (Security by Design)	Horizontale Cybersicherheitsanforderungen für Hardware/Software mit digitalen Elementen	**Inkrafttreten:** 10.12.2024 **Geltungsbeginn:** 11.12.2027 (Meldepflichten ab 09/2026)
DORA VO (EU) 2022/2554	**Art. 5-16** (IKT-Risikomanagement) **Art. 17-23** (Vorfallsmeldung)	Digitale operationale Widerstandsfähigkeit im Finanzsektor und bei IKT-Dienstleistern	**Inkrafttreten:** 16.01.2023 **Geltungsbeginn:** 17.01.2025
DGA (Data Governance Act) VO (EU) 2022/868	**Art. 12** (Datenvermittlung) **Art. 18** (Datenaltruismus)	Vertrauenswürdige Strukturen und sichere Vermittler für das Datenteilen in Europa	**Inkrafttreten:** 23.06.2022 **Geltungsbeginn:** 24.09.2023
Data Act (Datenverordnung) VO (EU) 2023/2854	**Art. 10** (Streitbeilegung) **Art. 13** (Missbräuchliche Verträge)	Rechte zum Datenzugang (z. B. IoT) und Schutz vor wirtschaftlicher Übervorteilung im B2B	**Inkrafttreten:** 11.01.2024 **Geltungsbeginn:** 12.09.2025
DSA (Digital Services Act) VO (EU) 2022/2065	**Art. 16** (Notice & Action) **Art. 25** (Dark Patterns) **Art. 26/28** (Werbeverbote)	Verantwortung für Inhalte, Bekämpfung illegaler Inhalte und Schutz der Grundrechte online	**Inkrafttreten:** 16.11.2022 **Geltungsbeginn:** 17.02.2024
DMA (Digital Markets Act) VO (EU) 2022/1925	**Art. 3** (Gatekeeper-Status) **Art. 5-7** (Verhaltenspflichten & Interoperabilität)	Faires Wettbewerbsumfeld, Brechen der Marktmacht der riesigen „Gatekeeper"-Konzerne	**Inkrafttreten:** 01.11.2022 **Geltungsbeginn:** 02.05.2023
AI Act (KI-Verordnung) VO (EU) 2024/1689	**Art. 5** (Verbotene KI) **Art. 6/10/15** (Hochrisiko-KI) **Art. 50/51** (Transparenz/ GPAI)	Produktsicherheit für KI-Systeme auf Basis eines strikt risikobasierten Ansatzes	**Inkrafttreten:** 01.08.2024 **Geltungsbeginn:** 02.08.2026 (stufenweise Vorab-Fristen ab Frühjahr 2025)

Abbildung 2: Quelle: Bild generiert von Gemini (Google AI)

Quellen:

[1] Europäische Kommission (2020): Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Gestaltung der digitalen Zukunft Europas. COM(2020) 67 final. In: eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020DC0067

[2] Europäische Kommission (2020): Gemeinsame Mitteilung an das Europäische Parlament und den Rat: Die EU-Strategie für Cybersicherheit für die digitale Dekade. JOIN(2020) 18 final. In:https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020JC0018

[3] Europäische Kommission (2020): Europa für das digitale Zeitalter: neue Vorschriften für digitale Plattformen. Pressemitteilung (IP/20/2347) vom 15. Dezember 2020. In: https://static.hospitalityinside.com/image/convert/hos/2023/06/15/article-3-eu-digital-regeln-fuer-plattformen-dez-2020-648a78379be9e924498144.pdf?s=7991da587ae734180a7182445a70317d

[4] Europäische Kommission (2020): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte). COM(2020) 842 final. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0842&from=el

[5] Europäische Kommission (2020): Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie. COM(2020) 66 final. In: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020DC0066

[6] Europäische Kommission (o.J.): Ein Europa für das digitale Zeitalter. Eine neue Generation von Technologien für die Menschen. In: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_de

[7] Europäische Union (2016): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). In: Amtsblatt der Europäischen Union, L 119. In: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] Europäische Union (2022): Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333 vom 27.12.2022. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

[9] Europäische Union (2024): Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 sowie der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. L, 2024/2847 vom 20.11.2024. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402847

[10] Europäische Union (2022): Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (DORA-Verordnung), ABl. L 333 vom 14.12.2022. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

[11] Zippelius, Reinhold: Juristische Methodenlehre, 11. Auflage, Verlag C.H. Beck, München 2012, Kapitel II, §7c.

[12] Europäische Kommission (o.J.): Datengesetz. In: https://digital-strategy.ec.europa.eu/de/policies/data-act

[13] Europäische Union (2022): Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) Nr. 2018/1724 (Daten-Governance-Rechtsakt), ABl. L 152/1 vom 3.6.2022. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R0868

[14] Europäische Union (2023): Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) Nr. 2017/2394 und der Richtlinie (EU) Nr. 2020/1828 (Datenverordnung), ABl. L vom 22.12.2023. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202302854

[15] Europäische Union (2022): Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277/1 vom 27.10.2022. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2065

[16] Europäische Union (2022): Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. L 265/1 vom 12.10.2022. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R1925

[17] Europäische Union (2016): Vertrag über die Arbeitsweise der Europäischen Union (Konsolidierte Fassung), ABl. C 202/1 vom 7.6.2016. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12016E/TXT

[18] Europäische Union (2024): Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L vom 12.7.2024. In: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689

[19] Bradford, Anu (2020): The Brussels Effect: How the European Union Rules the World. Oxford University Press. https://academic.oup.com/book/36491?__cf_chl_f_tk=tKMCbsbrXRpph3.AkI6WfC3Sz28fMHGx-bZxAiS.P6Y0-1783068351-1.0.1.1-F_OsIsb5cAsPR_toXiwfAnx0LdS_iuwMYJDHIHsPmWs

Alexander Lewisch ist Consultant bei SEQIS.

Als IT-Quereinsteiger und Wiedereinsteiger konnte er Erfahrungen im Software Testing sammeln und Einblicke in diverse Bereiche wie Testmanagement, Testdurchführung, Testautomation, Testkoordination, Reporting und Consulting sammeln.

Derzeit widmet er sich verschiedenen Testprojekten im Bereich der Remote Testing Services (RTS).

Vertrauen & radikale Transparenz als härteste Währung im IT-Projektmanagement

von Melanie Gau

In der hypervernetzten globalen Wirtschaft ist Vertrauen längst kein „Softskill" mehr, sondern hat sich zu einer harten ökonomischen Kennzahl entwickelt. Während früher Kapital oder Rohstoffe Märkte dominierten, entscheidet in der Ära der digitalen Transformation der „Digital Trust" über Erfolg und Misserfolg. Dieser Artikel analysiert, wie IT-Projektleiter*Innen durch radikale Ehrlichkeit, datengesteuerte Führung und psychologische Sicherheit Krisen in strategische Assets verwandeln können.

Wenn Projekte wanken...

In einer idealen Welt verlaufen IT Projekte linear vom Kick-off zum Go-live. Die Realität ist jedoch von Komplexität, Veränderung, Budgetüberschreitungen und technischen Fehlern geprägt. An diesem Punkt fungiert eine Krise als ultimativer Stresstest für das Vertrauensverhältnis zwischen Projektteam und Stakeholder*Innen.

Studien zeigen, dass Organisationen, die im Bereich Digital Trust führen, eine 1,6-mal höhere Wahrscheinlichkeit für signifikantes Umsatzwachstum aufweisen[1]. Vertrauen wirkt hierbei wie ein Beschleuniger: In High-Trust-Umgebungen steigen die Entscheidungsgeschwindigkeit und Effizienz, während die Kosten für Kontrolle sinken. Umgekehrt wirkt fehlendes Vertrauen wie eine „Steuer" auf jede Kommunikation.

Das Ende der „Watermelon-Reports"

Ein kritisches Hindernis für Digital Trust ist der „Watermelon-Effect"[2]: Projekte, die in Dashboards nach außen „grün" erscheinen, im Kern jedoch bereits tief „rot" gefärbt sind. Dieses Phänomen ist oft das Resultat einer toxischen Unternehmenskultur, in der Manager*Innen befürchten, dass ein kritischer Status als persönliches Versagen gewertet wird.

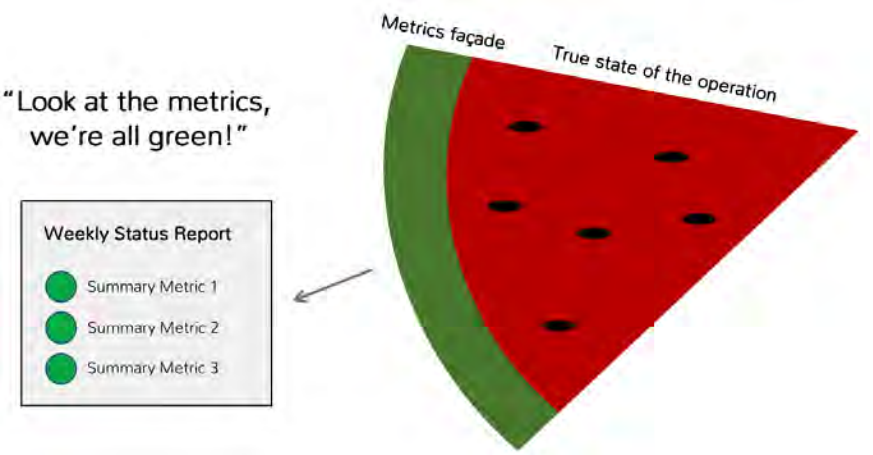


Abbildung 1 „Watermelon Effect": Quelle: https://ckmanalytix.com/beware-of-the-watermelon/

Um diese „grüne Schale" aufzubrechen, muss seitens der Führungsebene aktiv der Preis der Wahrheit gesenkt werden.

Praktische Maßnahmen:

- Meetings sollten **gezielt nach Blockaden fragen**, statt nur Erfolge zu feiern.
- Aufgaben gelten nur als **0% oder 100% fertig**, um die „90%-Falle" zu vermeiden.
- Die **frühzeitige Eskalation** von Risiken wird belohnt, statt bestraft.

KPIs statt Bauchgefühl

Um die Subjektivität aus Krisengesprächen zu nehmen, ist der Übergang zu einer datengestützten Führung unerlässlich. Valide Metriken dienen als objektive Schiedsrichter. Ein zentrales Beispiel ist die mathematische Bestimmung der **Fehlerdichte**, also die „Anzahl der in der Software/im Modul bestätigten Fehler während einer bestimmten Zeit im Betrieb bzw. der Entwicklung geteilt durch den Nutzungsumfang der Software/des Moduls"[3].
Neben dieser Softwarequalität sind Kennzahlen wie die **Sprint Velocity** (Lieferfähigkeit: Misst die Menge an Arbeit, die ein Team innerhalb einer festen Zeitspanne erfolgreich abschließt) und die **Change Failure Rate** (Änderungsfehlerrate: Definiert den Prozentsatz der Änderungen, die in der Produktion zu Fehlern, Ausfällen oder Störungen führen und Nachbesserung erfordern) geeignet, um die Kontrolle über die technische Realität nachzuweisen.

Durch eine möglichst früh erstellte Kombination aus Metriken und Analyse kann man damit während eines Projekts besser den Überblick bewahren und auf Vorkommnisse reagieren:

Abbildung 2: Quelle: Bild generiert von Gemini (Google AI)

Psychologische Sicherheit als menschliches Fundament

Technologische Exzellenz entfaltet ihre Wirkung nur in einem Klima der psychologischen Sicherheit. Amy Edmondson, Management-Wissenschaftlerin an der Harvard Business School, definiert dieses bahnbrechende Konzept als die Gewissheit, dass man für das Äußern von Sorgen nicht gedemütigt wird[4]. Teams mit hoher psychologischer Sicherheit erkennen Fehler schneller und kommunizieren diese offen, was die Gesamtkosten der Fehlerbehebung senkt. Dies ist der Kern des Digital Trust: Die Integrität des menschlichen Systems hinter der Technologie.

Aktives Change Management[5]

Wenn Veränderungen stattfinden, greift das ADKAR-Modell6, um StakeholderInnen durch den Veränderungsprozess zu führen:
Echter Digital Trust entsteht durch Partizipation: StakeholderInnen sollten aktiv in die Lösungsfindung einbezogen werden, z.B. durch gemeinsame Steuerungsgremien.

Fazit

„In einer Zeit des Wandels ist die größte Währung das Vertrauen, das die Menschen in eine Führungskraft setzen."[7] — Stephen M. R. Covey

Vertrauen ist das größte Kapital für ManagerInnen in Zeiten der Unsicherheit. Transparenz ist dabei kein Akt der Schwäche, sondern ein Beweis für Reife und Kompetenz. Wer bereit ist, die „rote Innenseite" seiner Projekte offen zu legen und auf Daten statt auf das Bauchgefühl setzt, schafft die Voraussetzung für langfristigen Erfolg.

So paradox es auch klingen mag:

> In einer Welt, in der Qualität die Währung ist, bleibt **Transparenz der sicherste Tresor**.

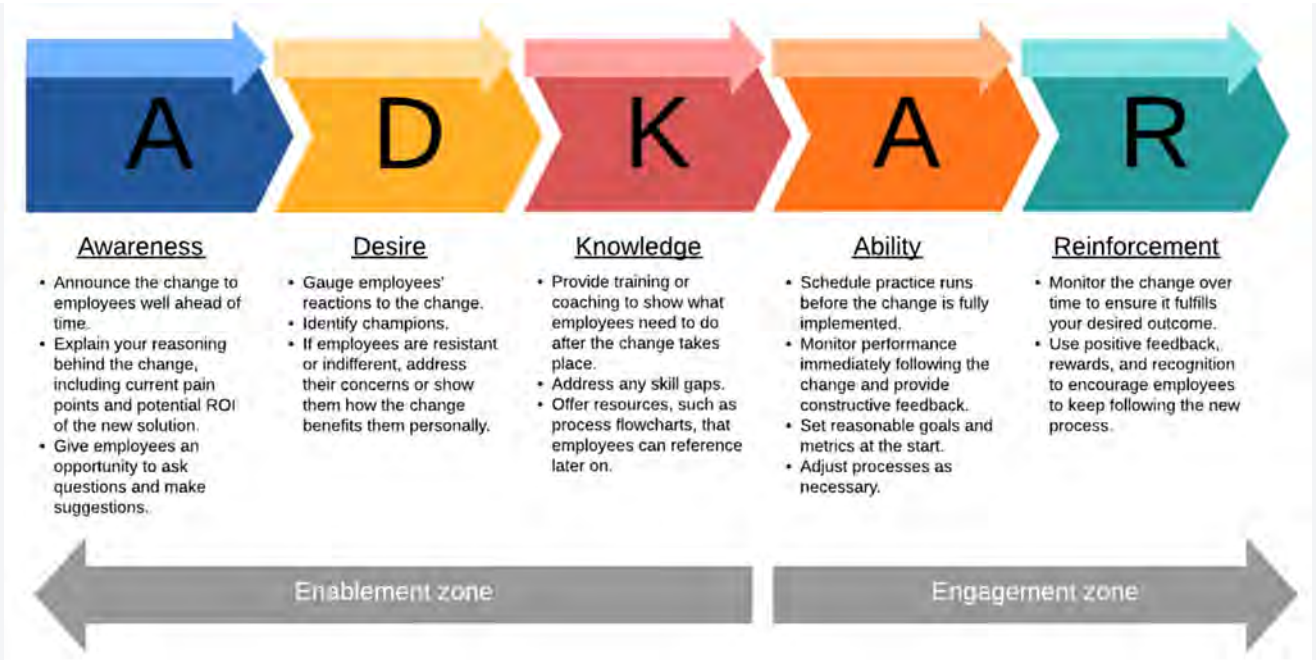


Abbildung 3: ADKAR Modell
Quelle: https://lucid.co/de/blog/verwendung-des-adkar-modells-fuer-change-management

Quellen und weiterführende Literatur

[1] McKinsey: https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters (Zugriff 12.03.2026)

[2] Nicholas Hartman: https://ckmanalytix.com/beware-of-the-watermelon/ (Zugriff 11.04.2026)

[3] Amy C. Edmondson: https://amycedmondson.com/category/psychological-safety/ (Zugriff 12.03.2026)

[4] Thomas Hamilton: https://www.guru99.com/de/defect-density-software-testing-terminology.html (Zugriff 11.04.2026)

[5] Alexander "weixi" Weichselberger: https://www.seqis.com/de/events/change-management-in-projekten-darauf-kommt-es-an?day=20220324&times=1648076400%2C1648162799

[6] Lucidchart: https://lucid.co/de/blog/verwendung-des-adkar-modells-fuer-change-management (Zugriff 11.04.2026)

[7] Stephen Covey: https://www.youtube.com/watch?v=igyxxYShXYo (Zugriff 12.03.2026)

Melanie Gau ist Senior Consultant bei SEQIS.

Ihr Steckenpferd ist die reibungslose Realisierung von IKT Projekten, und zwar von der Geburt einer innovativen Idee bis zur erfolgreichen Markteinführung. Sie verbindet technisches Know-How mit enger Kommunikation mit allen an einer gelungenen Umsetzung Beteiligten, stets mit Blick auf angemessenes, wirtschaftsorientiertes Management. Sie hat eine ganz persönliche Liebe zu agilen Methoden und der Aktivierung von Potentialen für die Herausforderungen im Zeitalter von Industrie 4.0.


IT PingPong
AI-Specials
Jetzt anhören!
Überall da, wo
es Podcasts gibt.
IT PingPong
DeepSeek & LLMs:
Was steckt
dahinter?
IT PingPong
Artificial
Intelligence
im Fokus
IT PingPong
AI-Agenten:
Digitale Helfer
im Alltag
IT PingPong
AI Act-Klartext
Was kommt auf
uns zu?
IT PingPong
AI 101
for everyone
Zu den Folgen:

Datensouveränität in Zeiten generativer KI: Warum nur eine lokale Lösung die richtige Antwort ist

von Alexander Vukovic

Abbildung 1: Quelle: Bild generiert von AI

1. Das Dilemma: Intelligenz gegen Kontrolle

Es gibt einen Satz, der in fast jeder Vorstandsetage fällt, wenn es um künstliche Intelligenz geht: „Ja, aber was passiert mit unseren Daten?" Und zum ersten Mal in der Geschichte der IT-Innovationen ist diese Frage nicht nur berechtigt — sie ist existenziell.

Generative KI hat in den letzten zwei Jahren eine technologische Revolution ausgelöst, die in ihrer Geschwindigkeit und Tragweite beispiellos ist. Modelle wie GPT-4, Claude oder Gemini können Code schreiben, Verträge analysieren, Testfälle generieren und Geschäftsstrategien bewerten. Sie sind brillant. Und sie sind gefährlich — nicht weil die Technologie per se schädlich wäre, sondern weil ihr dominantes Betriebsmodell auf einem fundamentalen Tausch basiert: **Intelligenz gegen Kontrolle.**

Wenn Sie heute ChatGPT Enterprise oder GitHub Copilot nutzen, dann schicken Sie Ihren proprietären Source-Code, Ihre internen Dokumente, Ihre Kundendaten und Ihre Geschäftsstrategien an Server, die Sie weder kontrollieren noch auditieren können. Die Anbieter versprechen Datenschutz. Die Verträge enthalten Klauseln. Aber die physische Realität bleibt: Ihre Daten verlassen Ihr Unternehmen, passieren internationale Netzwerke und werden auf Hardware verarbeitet, die jemand anderem gehört.

Für viele Unternehmen — insbesondere in regulierten Branchen wie Finanzdienstleistungen, Gesundheitswesen, Energie und öffentliche Verwaltung — ist das keine akzeptable Grundlage für eine KI-Strategie.

2. Was „Datensouveränität" wirklich bedeutet

Datensouveränität ist mehr als ein Schlagwort und mehr als Datenschutz. Es ist ein Dreiklang aus drei unverhandelbaren Prinzipien:

- **Meine Daten.** Ich bestimme, welche Daten erhoben und verarbeitet werden. Keine implizite Einwilligung durch AGB-Klauseln. Keine „anonymisierten" Telemetriedaten, die in aggregierter Form doch Rückschlüsse auf mein Unternehmen zulassen.
- **Meine Regeln.** Ich bestimme die Verarbeitungslogik, die Aufbewahrungsfristen und die Zugriffsrechte. Wenn ich entscheide, dass mein Source-Code niemals ein bestimmtes Netzwerksegment verlassen darf, dann ist das keine Empfehlung — das ist eine Architekturentscheidung mit bindender Wirkung.
- **Mein Eigentum.** Das, was die KI aus meinen Daten generiert — ob Testfälle, Analysen oder refactored Code — gehört mir. Vollständig. Ohne dass ein Cloud-Anbieter implizit Trainingsrechte an den Input- oder Output-Daten beanspruchen könnte.

Dieser Dreiklang klingt selbstverständlich. In der Praxis scheitert er an der Architektur der meisten KI-Lösungen am Markt.

3. Warum die Cloud das Problem ist — nicht die Lösung

Lassen Sie mich das konkret machen. Betrachten wir drei typische Szenarien:

Szenario 1: Code-Review mit Cloud-KI Ein Entwickler kopiert eine Klasse aus dem internen ERP-System in ein Cloud-basiertes KI-Tool, um einen Code-Review durchzuführen. In diesem Moment verlässt die Geschäftslogik — Pricing-Algorithmen, Rabattstaffeln, Kundenklassifizierungen — das Unternehmen. Selbst wenn der Anbieter die Daten nicht speichert: Während der Verarbeitung liegen sie im RAM eines Servers, der Ihnen nicht gehört. Ein Sicherheitsvorfall beim Anbieter, eine staatliche Anfrage (CLOUD Act, FISA) oder ein kompromittierter Mitarbeiter — und

Ihr wertvollstes Asset ist exponiert.

Szenario 2: Testdatengenerierung mit personenbezogenen Daten
Ein Testteam benötigt realistische Testdaten für eine Versicherungsanwendung. Die einfachste Methode: Produktionsdaten anonymisieren und in die Cloud-KI laden, um Varianten zu erzeugen. Problem: Die Anonymisierung ist nie perfekt. Re-Identifikationsrisiken bestehen immer. Und der Upload in eine Cloud-KI ist eine Datenübermittlung im Sinne der DSGVO — mit allen Konsequenzen.

Szenario 3: Strategische Analyse
Die Geschäftsführung möchte eine KI nutzen, um Wettbewerbsanalysen, M&A-Szenarien oder Markteintrittsstrategien zu modellieren. Dass diese Informationen in der Cloud eines US-amerikanischen Tech-Konzerns landen, ist nicht nur ein Datenschutzproblem. Es ist ein Wettbewerbsrisiko.

In jedem dieser Fälle gibt es eine gemeinsame Lösung: **Die Intelligenz muss zu den Daten kommen — nicht umgekehrt.**

4. Der regulatorische Druck: AI Act und DSGVO als Beschleuniger

Wer glaubt, dass Datensouveränität eine freiwillige Kür ist, unterschätzt den regulatorischen Druck, der sich aufgebaut hat.

Der EU AI Act, seit August 2024 in Kraft, klassifiziert KI-Anwendungen in Risikoklassen. Für Hochrisiko-Anwendungen — und dazu gehören viele Unternehmensanwendungen in den Bereichen HR, Kreditwesen und kritische Infrastruktur — gelten strenge Transparenz-, Dokumentations- und Governance-Anforderungen. Wer einen Cloud-Dienst nutzt, dessen Modell er nicht einsehen, nicht auditieren und nicht kontrollieren kann, wird Schwierigkeiten haben, diese Anforderungen zu erfüllen.

Die DSGVO bleibt das Fundament des europäischen Datenschutzes. Artikel 28 (Auftragsverarbeitung) und Artikel 44ff (Drittlandtransfer) stellen hohe Hürden für die Nutzung von Cloud-KI-Diensten, insbesondere wenn diese auf US-Infrastruktur laufen. Das Data Privacy Framework (DPF) bietet zwar einen Rechtsrahmen, aber seine Haltbarkeit ist — nach den Erfahrungen mit Safe Harbor und Privacy Shield — fragil.

NIS2 verschärft die Anforderungen an die IT-Sicherheit in kritischen Sektoren. Die Nutzung externer KI-Dienste für sicherheitsrelevante Aufgaben muss im Risikomanagement berücksichtigt und dokumentiert werden.

Die Botschaft ist klar: Regulierung belohnt Kontrolle.

Und Kontrolle bedeutet: lokal.

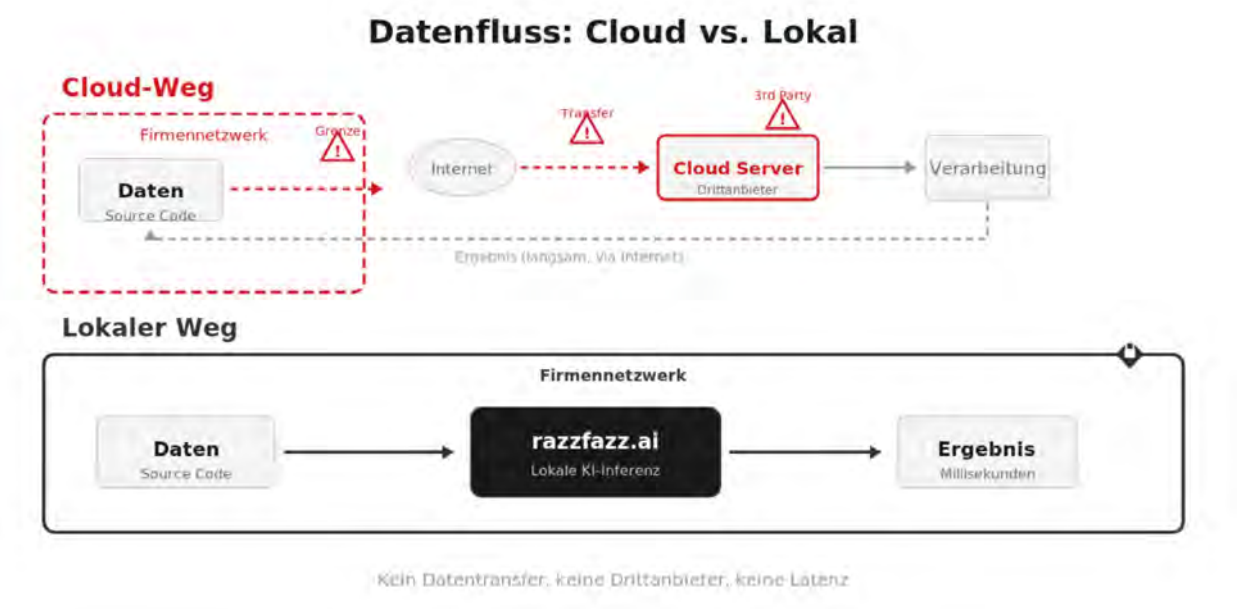


Abbildung 2: Datenreise-Diagramm: Cloud-Weg vs. lokaler Weg
Quelle: Bild generiert von AI

Abbildung 3: Regulatorik-Übersicht: EU AI Act, DSGVO, NIS2
Quelle: Bild generiert von AI

5. Die technologische Antwort: Warum lokale KI heute funktioniert

Noch vor zwei Jahren war „lokale KI" ein Synonym für „langsam und dumm". Die Modelle, die auf Consumer-Hardware liefen, waren bestenfalls für Spielereien geeignet. Diese Zeiten sind vorbei.

Drei technologische Entwicklungen haben die Situation grundlegend verändert:

Unified Memory Architecture: Moderne Hardware — auf der auch die razzfazz.ai Box basiert — beseitigt den klassischen Flaschenhals zwischen CPU und GPU. CPU und GPU teilen sich einen gemeinsamen Speicherpool von bis zu 128 GB. Das bedeutet: Kein Kopier-Overhead, kein VRAM-Engpass, keine Leistungseinbrüche bei großen Modellen. Wir können quantisierte Versionen von Modellen mit 70 Milliarden Parametern oder mehr lokal betreiben — in normalen Büroumgebungen, ohne Serverraum, bei einem Energieverbrauch von 30 bis 300 Watt.

Hocheffiziente Open-Source-Modelle: Die Open-Weights-Bewegung hat Modelle hervorgebracht, die mit proprietären Cloud-Diensten konkurrieren können. Magistral (Mistral AI) ist ein dediziertes Reasoning-Modell, das komplexe logische Aufgaben durch Chain-of-Thought-Analyse löst. Devstral (ebenfalls Mistral AI) ist auf agentische Software-Engineering-Tasks spezialisiert. Qwen3-Coder-Next (Alibaba) liefert herausragende Ergebnisse bei der Code-Generierung und -Analyse. All diese Modelle sind Open Source, lokal betreibbar und auditierbar.

Quantisierung ohne Qualitätsverlust: Durch Techniken wie 4-Bit- und 8-Bit-Quantisierung (GGUF-Format) wird der Speicherbedarf massiv reduziert, bei vernachlässigbarem Qualitätsverlust. Was vor zwei Jahren einen 50.000-Euro-GPU-Cluster erforderte, läuft heute auf einer kompakten Box auf Ihrem Schreibtisch.

6. Die razzfazz.ai Box: Datensouveränität als Architekturprinzip

Mit razzfazz.ai haben wir bei SEQIS keine eigene „KI" entwickelt. Wir haben etwas Wichtigeres getan: Wir haben eine **Plattform geschaffen, die es Unternehmen ermöglicht, beliebige Open-Source-KI-Modelle souverän und sicher zu betreiben.**

Die Box ist ein gehärtetes Linux-System (Ubuntu 24.04 LTS) mit einer integrierten Software-Suite:

- **llama.cpp** als hocheffiziente Inferenz-Engine für quantisierte Modelle
- **Workflow Automation** für die Orchestrierung von KI-Agenten (vergleichbar mit n8n, aber lokal und containerisiert)
- **PostgreSQL + pgVector** als lokale Vektordatenbank für RAG-Systeme (Retrieval Augmented Generation)
- **Open WebUI** als benutzerfreundliche Oberfläche mit Multi-User-Support
- **Docker-Container** für isolierte, reproduzierbare Deployments

Abbildung 4: Quelle: razzfazz.ai

Das Entscheidende: Jede Komponente läuft lokal. Es gibt keinen „Phone-Home"-Mechanismus, keine Telemetrie, keinen Cloud-Fallback. Die Box kann — wenn gewünscht — in einem vollständig air-gapped Netzwerk betrieben werden. Kein Internet, keine Exposition, maximale Kontrolle. Proceedings für Offline Updates werden mitgeliefert.

Was die Box in der Praxis leistet
Die Anwendungsfälle sind vielfältig und branchenübergreifend:

- **Für Entwicklungsteams:** Automatisierte Code-Reviews, Unit-Test-Generierung, Legacy-Code-Modernisierung, API-Testdesign — alles ohne dass eine Zeile Code das Firmennetzwerk verlässt.
- **Für Testteams:** DSGVO-konforme synthetische Testdatengenerierung, intelligente Testfallableitung aus Anforderungen, Self-Healing-Testsuiten, die sich an Code-Änderungen anpassen.
- **Für das Management:** Strategische Analysen, Dokumentenauswertung, Knowledge-Management — auf Basis eines lokalen RAG-Systems, das auf Ihre internen Fachkonzepte, Wikis und Testpläne zugreift.
- **Für Compliance-Verantwortliche:** Volle Transparenz über das verwendete Modell (Open Source, auditierbar), keine Drittlandtransfers, keine Auftragsverarbeitung, vollständige Kontrolle über Input und Output.

7. Der Kostenvergleich: Warum „lokal" günstiger ist, als Sie denken

Ein verbreitetes Vorurteil: „Die Cloud ist doch billiger — ich zahle nur, was ich nutze." Das stimmt für einfache Anfragen. Für Reasoning-Modelle und agentische Workflows, die tausende Tokens pro Anfrage generieren, dreht sich die Rechnung schnell um.

Die Box amortisiert sich bei intensiver Nutzung durch ein Entwicklerteam typischerweise innerhalb weniger Monate. Und sie hat einen psychologischen Effekt, der nicht zu unterschätzen ist: Wenn die KI „kostenlos" ist (weil bereits bezahlt), nutzen Entwickler sie häufiger, experimentieren mehr und integrieren sie tiefer in ihre Workflows.

Ihr Weg zur lokalen AI

- **Premium KI-Qualität aus Europa**
- **100 % unabhängig von Drittanbietern**
- **DSGVO- & AI-Act konform**

www.razzfazz.ai

Kostenvergleich: Cloud AI vs. Local AI (razzfazz.ai Box)

Kategorie	Cloud AI	razzfazz.ai Box
Reasoning / Denkzeit	Teuer Pro Token abgerechnet	Kostenlos Lokale Berechnung
Code-Scan großer Kontext	Sehr teuer Große Kontextfenster	Kostenlos Unbegrenzter Kontext
Wiederkehrende Tasks	Linear steigend Jede Ausführung kostet	Fixkosten Einmalige Investition
Datentransfer	Kosten + Risiko Daten verlassen Firma	Kein Transfer Alles bleibt intern

Abbildung 5: Kostenvergleich: Cloud AI vs. Local AI
Quelle: Bild generiert von AI

8. Fazit: Meine Daten, meine Regeln, mein Eigentum

Die KI-Revolution wird nicht aufzuhalten sein. Aber wie wir sie gestalten, liegt in unserer Hand. Die Frage ist nicht ob wir KI nutzen, sondern **wo und unter welchen Bedingungen.**

Datensouveränität ist kein Luxus und keine Bremse. Sie ist eine Architekturentscheidung, die Unternehmen langfristig handlungsfähig hält. Sie ist die Grundlage dafür, dass Innovation und Compliance kein Widerspruch sein müssen.

Die Technologie ist reif. Unified Memory Hardware, Open-Source-Modelle und intelligente Orchestrierung machen lokale KI heute praxistauglich, leistungsfähig und wirtschaftlich. Die razzfazz.ai Box ist der Beweis.

Warten Sie nicht darauf, dass die Cloud sicherer wird. Holen Sie sich die Kontrolle zurück. Denn am Ende geht es nicht um Technologie. Es geht um ein Grundprinzip, das so alt ist wie das Eigentum selbst:

Meine Daten.
Meine Regeln.
Mein Eigentum.

Quellen und weiterführende Informationen:

- EU AI Act – Verordnung (EU) 2024/1689, https://eur-lex.europa.eu/eli/reg/2024/1689
- DSGVO – Verordnung (EU) 2016/679, https://dsgvo-gesetz.de/
- NIS2-Richtlinie – Richtlinie (EU) 2022/2555
- razzfazz.ai – Lokal. Open Source. Unabhängig. Sicher., https://razzfazz.ai/
- SEQIS – Ihre lokale AI Beratung, https://seqis.com/
- llama.cpp – High-performance LLM inference, https://github.com/ggml-org/llama.cpp
- Mistral AI – Magistral & Devstral, https://mistral.ai/
- Qwen3-Coder – Alibaba Cloud, https://huggingface.co/Qwen

Alexander Vukovic ist SEQIS Gründer und Chief Evangelist.

Er ist erster Ansprechpartner für alle agilen, testmethodischen und testtechnischen Anfragen. In der Praxis arbeitet er als AI Quality Coach, Berater, Interims-Testmanager, CI-Experte und Lasttester. Mehr als 25 Jahre Beratertätigkeit führten ihn während seiner zahlreichen Projekte in die unterschiedlichsten Branchen und Länder. Sein persönliches Motto: „Es gibt keine Probleme, sondern nur nicht gefundene Lösungen."

AI Development mit Qualität und Bewusstsein

von Klemens Loschy

Mit AI lässt sich mittlerweile ja ein großer Teil des Entwicklungs-Workflows unterstützen, wenn nicht sogar komplett umsetzen. Hinzu kommt, dass Applikationen nicht mehr ausschließlich von (erfahrenen) Entwickler:innen erstellt werden müssen, sondern dass mit der Hilfe der passenden AI-Agenten fast jeder dazu in der Lage ist: mit den richtigen Prompts oder Agenten purzeln sogar von Beginn an Testfälle heraus (die bei jeder Änderung verifiziert und erweitert werden), der Code wird statisch analysiert und natürlich compiliert, ein Security Check im Anschluss wird ebenfalls durchgeführt. Damit ist doch für die Qualität nachhaltig gesorgt, oder? Man könnte sogar argumentieren, dass so ein AI-Agent bessere Ergebnisse produziert als die meisten Junior-Entwickler:innen, und das auch noch um ein Vielfaches schneller. Daraus resultiert fast automatisch, dass von nun an ganz stark auf AI gesetzt werden muss, damit man konkurrenzfähig bleiben kann.

Wenn wir aber einen Schritt zurück gehen, sehen wir vielleicht, dass es einen Mittelweg zwischen "wir lassen nur noch die Agenten arbeiten" und "besser keine AI verwenden" geben muss. Aber schauen wir uns das gemeinsam im Detail an.

Die Junior-Falle

Dass viele AI-Agenten mit dem Fokus auf Software-Entwicklung besseren Code als Junior-Entwickler:innen schreiben und dafür wesentlich weniger Zeit brauchen, das kann man schon fast als gegeben annehmen. In jeder professionellen Software-Entwicklung braucht es aber jemanden, der den erstellten Code reviewed und gegebenenfalls auf besondere fachliche oder technische Anforderungen hin prüft - Senior-Entwickler:innen kommen hier ins Spiel. Es muss jemanden - und damit meine ich tatsächlich einen Menschen - geben, der den Überblick über das Projekt (aus einer technischen Perspektive) behält und technische Entscheidungen treffen darf und kann. Letztlich muss ja auch jemand aus technischer Sicht die Verantwortung über die Umsetzung übernehmen bzw. übernehmen können, da tut man sich aus jetziger Sicht noch schwer, diese Verantwortung auf einen AI-Agenten abzuwälzen (auch das kommt vielleicht noch).

Wir waren ja gerade dabei, die Arbeit unserer Junior-Entwickler:innen von AI Agenten machen zu lassen (weil schneller und vermutlich auch besser). Das bringt aber Konsequenzen mit sich, die man zumindest betrachten muss:

- Die Senior-Entwickler:innen müssen mehr Code reviewen und bewerten als ohne AI Unterstützung (denn der Output der AI-Agenten ist wesentlich höher)
- Die Rolle des Junior-Entwicklers, so wie sie bisher gelebt wurde, könnte dadurch obsolet werden
- Ohne diese Junior-Entwickler:innen, die viel Zeit in die vielen und immer mehr werdenden Aspekte der Softwareentwicklung gesteckt haben und zahlreiche Probleme lösen mussten, kann es zukünftig keine Senior-Entwickler:innen mehr geben
- Wenn es zukünftig aber (zumindest) weniger Senior-Entwickler:innen gibt, wer prüft dann den Code und übernimmt letztlich die technische Verantwortung?

Das skizziert natürlich das Worst-Case Szenario, aber vieles deutet aktuell darauf hin, dass diese Richtung zum Teil eingeschlagen wird.

Wer testet den Tester?

"Wie konnte der Fehler bis in die Produktion kommen, wir haben dafür doch einen Unit-Test?" - Hand hoch, wer noch nie einen Unit-Test gefunden hat, der falsch umgesetzt wurde oder die eigentlich notwendigen Prüfungen nicht (vollständig) umgesetzt hatte? Ein Unit-Test muss jedenfalls eines machen, bevor er ein guter Unit-Test überhaupt sein kann: er muss einmal fehlschlagen! Nur wenn geprüft wurde, dass der umgesetzte Unit-Test im Fehlerfall auch wirklich anschlägt, kann man sich mit hoher Wahrscheinlichkeit sicher sein, dass der Unit-Test auch bei einem tatsächlichen Fehlverhalten der getesteten Funktionalität anschlägt. Ein von Anfang an "grüner" Testfall sagt genau gar nichts aus.

Da kommt wieder das Review - oder im Test-Design auch "4 Augen Prinzip" genannt - ins Spiel: Testfälle müssen ebenfalls qualitätsgesichert werden! Wie immer gilt: ein risikobasierter Ansatz ist hier durchaus sinnvoll (wie fast immer in der QA). Man wird wohl nicht jeden Testfall Peer-Reviewen, aber die wesentlichen müssen geprüft werden. Die AI kann, wenn man sie richtig steuert, viele und natürlich auch gute Testfälle komplett automatisiert erstellen und durchführen, ich würde mich aber nicht darauf verlassen, ohne die Testfälle auch kritisch reviewed zu haben. Auch hier muss es fachlich und technisch gut ausgebildete menschliche Mitarbeiter geben, die diese Tätigkeiten jetzt, und auch in Zukunft übernehmen.

Die menschliche Aufsicht

Im EU-AI Act (Artikel 14) ist die menschliche Aufsicht bei Hochrisiko-Systemen vorgeschrieben. Jetzt kann man natürlich argumentieren,

dass nicht jedes System gleich als Hochrisiko-System eingestuft werden muss und dementsprechend diese vorgeschriebene Regel nicht immer anzuwenden ist, fair enough - auch hier wieder ein ganz klarer risikobasierter Ansatz. Und ja: wenn ich mir eine eigene kleine App Vibe-Code, dann werde ich deutlich weniger Wert auf Code-Qualität und Testabdeckung legen und auch mit etwaigen Fehlern leben können.

Aber auch bei nicht Hochrisiko-Systemen im kommerziellen Umfeld wird es problematisch, wenn durch Fehler im Produktivbetrieb z.B. personenbezogene Daten oder Anmeldedaten geleaked werden, denn (noch) haftet das Unternehmen und die Geschäftsführung bei derartigen Vorfällen und nicht die AI, die (vielleicht) den meisten Code dieser Systeme geschrieben hat.

Der "Social Media" Druck

Wenn man in den "Sozialen Medien" Beiträge über AI sieht, hört oder liest, dann bekommt man durchaus den Eindruck, dass diese Technologie unfehlbar ist: da werden Frameworks, Applikationen und ganze SaaS Plattformen in wenigen Stunden oder Tagen aus dem Boden gestampft. Erst vor Kurzem habe ich wieder einen Beitrag gesehen, in dem ein Entwickler meinte, dass sein AI-Agent, während er selbst geschlafen hat, seine Applikation umgesetzt hat (in nur 2 oder 3 Stunden), wofür ein Entwickler mehrere Tage gebraucht hätte. Was er nicht erzählt ist, wieviel Zeit er in die Analyse und Refactoring des Codes aufgewendet hat und welche Features unzureichend oder gar nicht umgesetzt wurden. Und verständlicherweise wird dadurch Druck auf die Unternehmen aufgebaut: "Alle anderen sind ja jetzt offensichtlich so viel schneller mit AI, also müssen wir da nachziehen". Und welche Tätigkeiten kann und konnte man immer schon kürzen? Richtig: Qualität! In Form von schlechter UX, mieser Performance oder ganz offensichtlichen Fehlern, die dann natürlich wieder von und mit AI gefixt werden (müssen), denn die Zeit sich einen Überblick über die Codebasis zu verschaffen, die hat sich keiner genommen.

AI: die "Silver Bullet"?

Wer erinnert sich noch an die 2000er, wo UI-Testautomation (damals noch mit Mercury WinRunner) aufkam und alle wie wild begonnen haben ihre Tests zu automatisieren? Dank "Capture/Replay" konnte da auch der Fachbereich fleißig mithelfen (so zumindest laut Mercury Werbung) - also die "Silver Bullet" um alle Qualitätsprobleme mit einem Schlag zu lösen! Ewig viel Zeit und Ressourcen sind daraufhin in den Aufbau und die Pflege solcher automatisierter Testfall-Portfolios geflossen und es hat einige Jahre gedauert, bis viele Unternehmen feststellen mussten, dass UI-Testautomation natürlich einen Mehrwert bringt, aber nur zielgerichtet in Maßen eingesetzt und als Ergänzung zu vielen anderen Test-Tätigkeiten, und schon gar nicht die "Silver Bullet" ist, als die sie einst dargestellt wurde.

Wie sollen wir also mit AI umgehen?

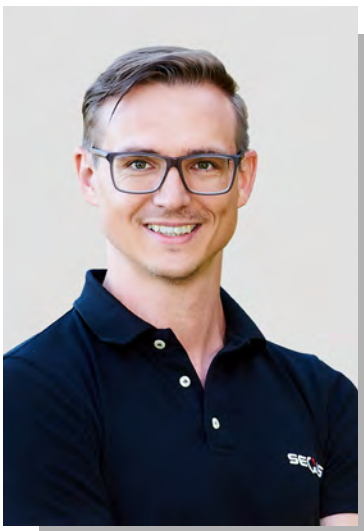
Aus meiner Sicht muss man AI als Werkzeug sehen: Werkzeuge haben sich seit jeher verbessert und damit die Produktivität, die Qualität und die Arbeitsweise maßgeblich verändert.

In den letzten Jahren haben wir ein neues Werkzeug in die Hand bekommen, mit dem wir erstmal lernen müssen richtig umzugehen. Aber wir Entwickler, Tester, allgemein wir Menschen sind immer noch diejenigen, die dieses Werkzeug verwenden und für das Ergebnis verantwortlich sind oder sein sollten! Aussagen wie "die AI hat gesagt" oder "keine Ahnung was der Code da genau macht, aber es funktioniert" haben in einer professionellen Software-Entwicklung einfach nichts zu suchen, jetzt nicht und auch nicht in der Zukunft! Software Development ist und bleibt ein immens anspruchsvolles Handwerk, das von gut ausgebildeten und erfahrenen Handwerkern durchgeführt wird.

Wir bei razzfazz.ai werden dieses neue Werkzeug natürlich zielgerichtet einsetzen, unsere Effizienz damit steigern aber unsere Grundwerte damit nicht über Bord werfen: wir erstellen qualitativ hochwertige, performante, sichere, gut bedienbare und getestete Produkte. Wir kennen unsere Code-Basis und übernehmen Verantwortung.

Quellen:

EU AI Act: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689



Klemens Loschy ist Mitglied des SEQIS Geschäftsleitungsteams und Principal Consultant.

Er kann auf jahrelange Erfahrung in den Bereichen Testautomation, Last-Tests und Performance Engineering, funktionale Tests, Testen in agilen Teams, Anwendungsentwicklung von Testsoftware sowie Beratung und Unterstützung in zahlreichen Projekten unterschiedlichster Branchen zurückblicken.

Es ist Webinar-Donnerstag!

Ten more things

- ✔ Praxisbezogene Fachvorträge zu aktuellen IT-Trendthemen
- ✔ Kompetentes, fachliches Know-how aus der Praxis
- ✔ 10 Tipps & Tricks für Ihren Arbeitsalltag
- ✔ Kostenlose Teilnahme
- ✔ Online

Termine

24. September 2026: Der Faktor Mensch im Zeitalter der KI – Warum Disziplin im Denken der Schlüssel zum Erfolg ist
12. November 2026: Interne Enterprise AI Governance-Strukturen operativ etablieren
April 2027: Thema tbd.
Juni 2027: Thema tbd.

Informiert bleiben

www.seqis.com/events-index

Warum digitales Vertrauen mit der Business Analyse beginnt

von Melanie Gau

In einer Ära, in der Software oft als undurchsichtige „Blackbox" wahrgenommen wird, reicht fehlerfreier Code allein nicht aus, um Vertrauen zu schaffen. Der Schlüssel zur digitalen Glaubwürdigkeit liegt in der Schnittstelle zwischen Mensch und Maschine. Hier agiert der Business Analyst als Brückenbauer, der durch klare Kommunikation, ethische Weitsicht und präzise Anforderungen das Fundament für echte Qualität und nachhaltiges Vertrauen legt.

Warum digitales Vertrauen mit der Business Analyse beginnt

In der heutigen digitalen Wirtschaft ist Vertrauen die Währung, die über den Erfolg oder Misserfolg von Produkten entscheidet. Wenn Endanwender ein System nicht verstehen oder Stakeholder das Gefühl haben, ihre Bedürfnisse wurden übergangen, erodiert der Digital Trust. Die Lösung für dieses Dilemma liegt nicht primär in der Programmierung, sondern in der vorgelagerten Phase: der Business Analyse. Der/die Business AnalystIn (BA) ist die Instanz, die das „Was" und „Warum" einer Softwarelösung definiert und erklärt.

Anforderungsklarheit als ultimativer Vertrauensbeweis

Ohne klare Anforderungen ist nicht definiert, was ein System beinhaltet. Unpräzise Requirements damit sind ein Risiko für digitale Integrität, da sie eine massive Lücke zwischen dem Erwartungsmanagement der Stakeholder und der gelieferten IT-Realität aufreißen. Ein BA sorgt dafür, dass diese Lücke geschlossen wird: Indem er/sie vage Wünsche in messbare, testbare und realistische Spezifikationen übersetzt, liefert er/sie den ersten und wichtigsten Vertrauensbeweis in einem IT-Projekt.

„Das Wichtigste an der Kommunikation ist, zu hören, was nicht gesagt wird." (Peter Drucker)

Oft äußern Fachabteilungen nur Symptome, nicht aber die eigentliche Ursache eines Problems. Die Übersetzung von „Business-Wunsch" in „IT-Machbarkeit" ist ein sensibler Prozess. Wenn Anforderungen nicht transparent erfasst werden, entstehen sogenannte „Shadow Requirements" – unausgesprochene Erwartungen oder versteckte Annahmen, die weder dokumentiert noch getestet werden. Solche blinden Flecken bergen ein enormes Risiko, denn sie führen zu Systemen, die zwar nach Spezifikation fehlerfrei laufen, aber im realen Betrieb versagen.

- Durch lückenlose und transparente Dokumentation (u.a. User Stories, Acceptance Criteria, Context Mapping, Event Storming) verhindert der BA, dass diese versteckten Risiken das Vertrauen der Endnutzer in der Produktionsumgebung unterwandern.
- Durch Stakeholder-Empathie, aktives Zuhören und institutionalisierte Rückkopplungsschleifen (z.B. Application Lifecycle Management) macht er den Prozess transparent und bindet die Nutzer aktiv in die Gestaltung ein.

Gleichzeitig gießt der BA diese Kommunikation in eine harte Währung für das IT-Testing: Die Definition of Done (DoD). Die DoD ist nichts Geringeres als ein handfestes Qualitätsversprechen. Indem der BA klare, testbare Akzeptanzkriterien formuliert, setzt er/sie die Leitplanken, an denen sich das spätere Testing messen lassen muss. Die Arbeit des BA liefert das exakte Koordinatensystem für das Testing, um zu verifizieren, ob die Software nicht nur richtig gebaut wurde (Verifikation), sondern ob auch das richtige System gebaut wurde (Validierung).

Abbildung 1: Quelle: Bild generiert von Gemini (Google AI)

Vertrauenswürdige KI ab der Konzeptionsphase

Mit dem zunehmenden Einsatz von KI bekommt die Rolle des BA eine neue, ethische Dimension. KI-Systeme gelten aufgrund ihrer Komplexität oft als die ultimativen Blackboxes. Hier trägt der BA die Verantwortung, eine ethische Basis zu schaffen. Die Vermeidung von kognitiven und datenbasierten Verzerrungen (Bias) darf erst gar nicht zum Problem der Entwickler oder Tester werden, sondern muss bereits in der Konzeptionsphase adressiert sein (Bias-Detection, Compliance-Framework). Der BA definiert die Parameter, nach denen KI-Entscheidungen nachvollziehbar, fair und transparent bleiben (Ethik by Design), und schützt so aktiv die Integrität des Systems.

Fazit

In der IT von heute ist Qualität die neue Währung und Digital Trust das Kapital. Der BA ist weit mehr als ein reiner Anforderungsverwalter; er/sie ist der Architekt der digitalen Glaubwürdigkeit. Durch die Kombination aus präzisem Requirements Engineering, ethischem Bewusstsein und tiefgreifender Kommunikation übersetzt er abstrakte Software in greifbare Werte. Nur wenn die Brücke zwischen Business-Bedürfnis, technischer Umsetzung und validierendem Testing stabil ist, entsteht Software, der Menschen wirklich vertrauen.

Quellen und weiterführende Literatur

Peter F. Drucker: The Essential Drucker, 2001

Edelman Trust Barometer: Jährliche, globale Studie zum Vertrauen von Konsumenten und Arbeitnehmern in Institutionen und Technologien
https://www.edelman.com/trust/trust-barometer

The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems: Ethically Aligned Design. Ein umfassendes Framework für die Integration von Ethik in der Entwicklung von KI-Systemen
https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/

Weitere Blogartikel von Melanie Gau:

Melanie Gau ist Senior Consultant bei SEQIS.

Ihr Steckenpferd ist die reibungslose Realisierung von IKT Projekten, und zwar von der Geburt einer innovativen Idee bis zur erfolgreichen Markteinführung. Sie verbindet technisches Know-How mit enger Kommunikation mit allen an einer gelungenen Umsetzung Beteiligten, stets mit Blick auf angemessenes, wirtschaftsorientiertes Management. Sie hat eine ganz persönliche Liebe zu agilen Methoden und der Aktivierung von Potentialen für die Herausforderungen im Zeitalter von Industrie 4.0.

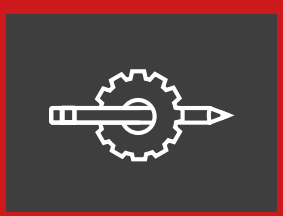
Die SEQIS Group ist der führende österreichische Anbieter für IT-Dienstleistungen mit Fokus auf **Artificial Intelligence, Softwaretest, IT-Analyse, Projektmanagement und individuelle Softwareentwicklung**. Zur Gruppe gehören die SEQIS GmbH und die razzfazz.ai GmbH.

IT Analyse

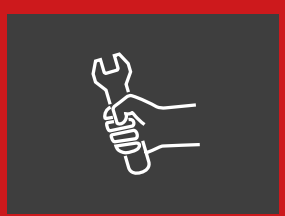
razzfazz.ai

Remote Testing Services

Release & Operate



DevOps



Methodology & Tools

Trainings & Workshops

Projekt-management

SEQIS.ai

AI. Analysis. Development. Test. Management. Better Results.
www.SEQIS.com
www.razzfazz.ai