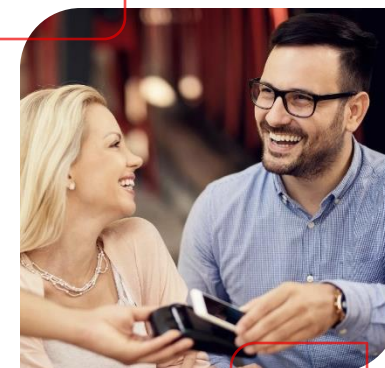


Wie kann Enterprise Architecture die Erfüllung regulatorischer Anforderungen unterstützen?

Challenge your Peers Session



Wir können #Zukunft.

Der Digitalisierungspartner der Sparkassen-Finanzgruppe.



**Wir sind der
Digitalisierungspartner
der Sparkassen
und einer der größten
IT-Dienstleister Europas.**

3 Standorte

5.400+ Mitarbeitende

2,7 Mrd. Euro Umsatz

450+ Mio. Euro Entwicklungsbudget

390.000+ betreute Endgeräte



Und betreiben alles sicher und
hochverfügbar im **größten**
Rechenzentrumsverbund für
Finanzdienstleistungen
in Deutschland und Europa.

38.700

Server

235.500

Terabyte
Speicherkapazität

84 Mio.

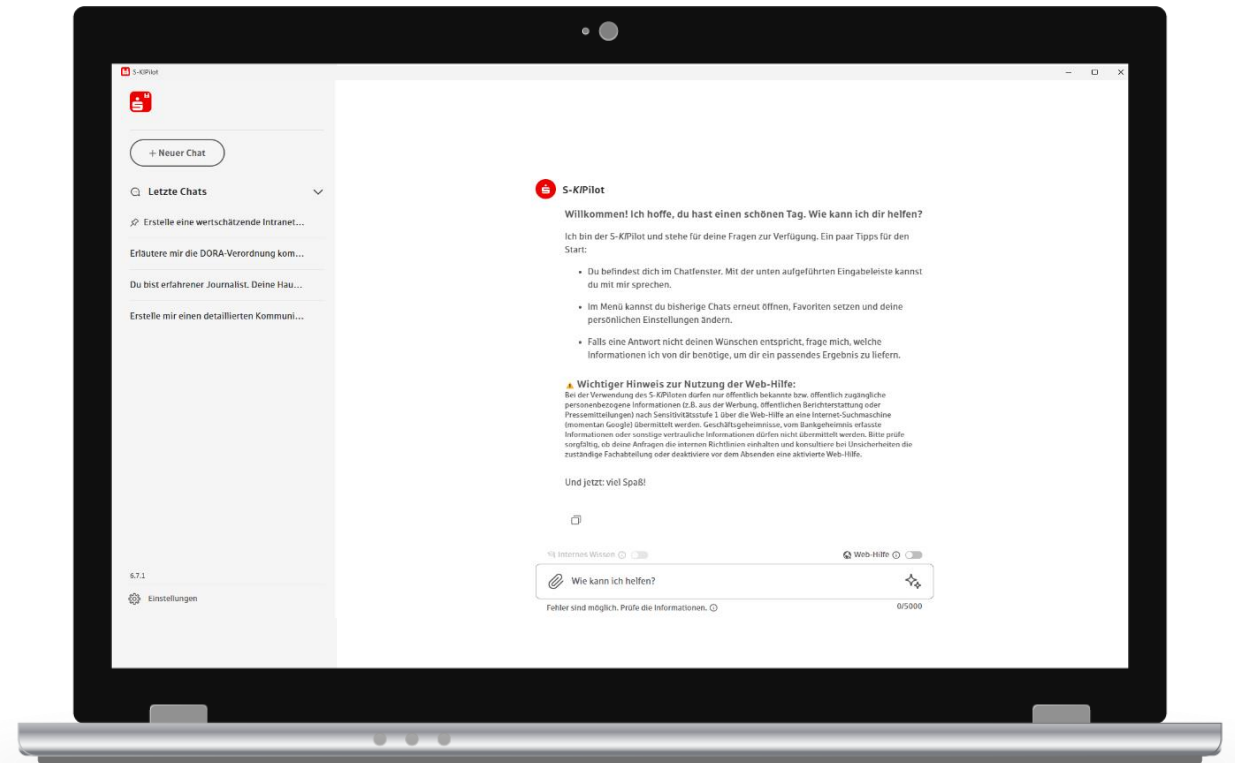
kWh
Ökostrom



Unsere KI-Strategie

stellt die digitale Souveränität der Sparkassen und den Schutz der Kundendaten sicher. Dank Open-Source-KI-Modellen in unseren Rechenzentren optimal auf die Sparkassen angepasst.

Der S-K/Pilot unterstützt am digitalen Arbeitsplatz



Challenge your Peers - Wie kann Enterprise Architecture die Erfüllung regulatorischer Anforderungen unterstützen?

Zwei Hebel, eine Verantwortungsfrage

Compliance & Governance aus Sicht eines IKT Dienstleisters im Bankensektor

Enterprise Architecture stützt die Regulatorik



Enterprise Architecture verbindet Geschäft, Anwendungen und Betrieb in einem einheitlichen Gesamtbild und macht regulatorische Anforderungen wie von DORA überhaupt erst prüffest.

KI unterstützt bei der Erfassung und Prüfung



Verantwortungsvolle KI erfasst, qualifiziert und pflegt Landschaften wenn Datenqualität und Nachvollziehbarkeit gesichert sind.

Kernfrage:

Wer verantwortet das Ergebnis, wenn eine KI regulatorische Governance prüft ?



Challenge your Peers - Wie kann Enterprise Architecture die Erfüllung regulatorischer Anforderungen unterstützen?

Vom Architekturmodell zum prüffesten Nachweis

EA als Hebel zur systematischen Erfüllung regulatorischer Anforderungen



EA kennt die Zusammenhänge zwischen Geschäftsfähigkeiten, Anwendungen und Infrastruktur. Genau diese Verbindung macht Anforderungen wie DORA prüffest. Dazu muss das Modell aber den realen Betrieb statt dem Wunschzustand abbilden.

- > Wie verknüpft ihr Lösungsarchitekturen mit dem realen Deployment (z.B.: CMDB, Infrastructure-as-Code, Runtime-Discovery)?
- > Soll-Architektur vs. Fortschreibung im Ist: Wie schließt ihr die Lücke ohne manuelle Dauerpflege?
- > Welche regulatorischen Nachweise erstellt ihr heute direkt mit dem EA-Repository / EA-Tooling?

Challenge your Peers - Wie kann Enterprise Architecture die Erfüllung regulatorischer Anforderungen unterstützen?

KI als Beitrag: Mit erforderlichlich hoher Datenqualität

Verantwortungsvoller KI-Einsatz ist nicht nur eine Frage der Ethik



KI kann System- und Anwendungslandschaften automatisch erfassen, qualifizieren und aktuell halten und so einen echten Beitrag zu EAM, Governance und Compliance leisten. Verantwortungsvoll wird er erst, wenn Konfidenz, Datenqualität und Nachvollziehbarkeit mitgeliefert werden.

- > Wo entlastet euch KI heute konkret (z.B.: Discovery, Klassifizierung, Verknüpfung, Dokumentation)?
- > Wie macht ihr Datenqualität und Konfidenz sichtbar (z.B.: Scoring, Human-in-the-loop, Stichproben)?
- > Wie stellt ihr sicher, dass KI-Daten nur nach inhaltlicher Prüfung (z.B. wegen Halluzinationen und falschen Quellangaben) in ein Compliance-Artefakt einfließen?

KI nicht als Allheillösung: Grenzen Kennen

Verantwortungsvoller KI-Einsatz ist nicht nur eine Frage der Ethik – Das bewusste „Nein“ zur KI



Verantwortungsvoller KI-Einsatz bedeutet, die eigenen Grenzen zu kennen. In regulatorisch sensiblen Entscheidungen kann der Verzicht auf KI die risikobewusste Wahl sein, insb. wenn eine manuelle Prüfung unerlässlich ist.

- > Wo zieht ihr bewusst die Grenze (z.B.: Finale Risikobewertung, kritisch wichtige Funktionen, Prüfarbefakte)?
- > Habt ihr Erfahrungen mit „Anti-KI“-Ansätzen oder bewusstem Nicht-Einsatz gemacht?
- > Was sind die Entscheidungskriterien für euch (z.B.: Deterministisch und erklärbar vs. KI-gestützt)?

Klare Zusammenarbeit mit geklärten Verantwortungen

Verantwortung muss stets in den Händen der Fachabteilungen bleiben



Nachhaltige Umsetzungen regulatorischer Anforderungen gelingen nur im Zusammenspiel von EA, Compliance und IT – ggf. jeweils KI gestützt. Je enger dieses Zusammenspiel, desto wichtiger wird die klare Zuordnung der Verantwortlichkeit

- > Wie ordnet ihr Verantwortlichkeiten zu (gibt es z.B. eine RACI-Matrix für regulatorische Anforderungen)?
- > Wer „besitzt“ den Compliance-Nachweis (z.B.: EA, Compliance oder IT-Betrieb)?
- > Wie verankert ihr Verantwortung dort, wo KI Entscheidungen vorbereitet (z.B.: Wird die Unterstützung durch KI dokumentiert? Geht ihr unterschiedlich mit internen vs. externen Modellen um?)?

**Vielen Dank für den
Austausch!**

Lasst uns gerne im Kontakt bleiben!

Dr. Dennis Horstkemper

Unternehmensarchitekt

dennis.horstkemper@f-i.de