



Effizient ist, wer eine gute Idee
mit einfachen Mitteln umsetzt.

Schutz und Verantwortung: Informations- & Cybersicherheit trifft auf Datenschutz

Eric S. Soong (Group Head Compliance & Corporate Security, Schaeffler Gruppe)
DACH-Compliance-Tagung 2025
27. März 2025

We pioneer motion

1

Governance Funktionen als „Independence Funktionen“

2

Compliance Management Systeme zur Handhabung aufkommender regulatorischer Vorgaben

3

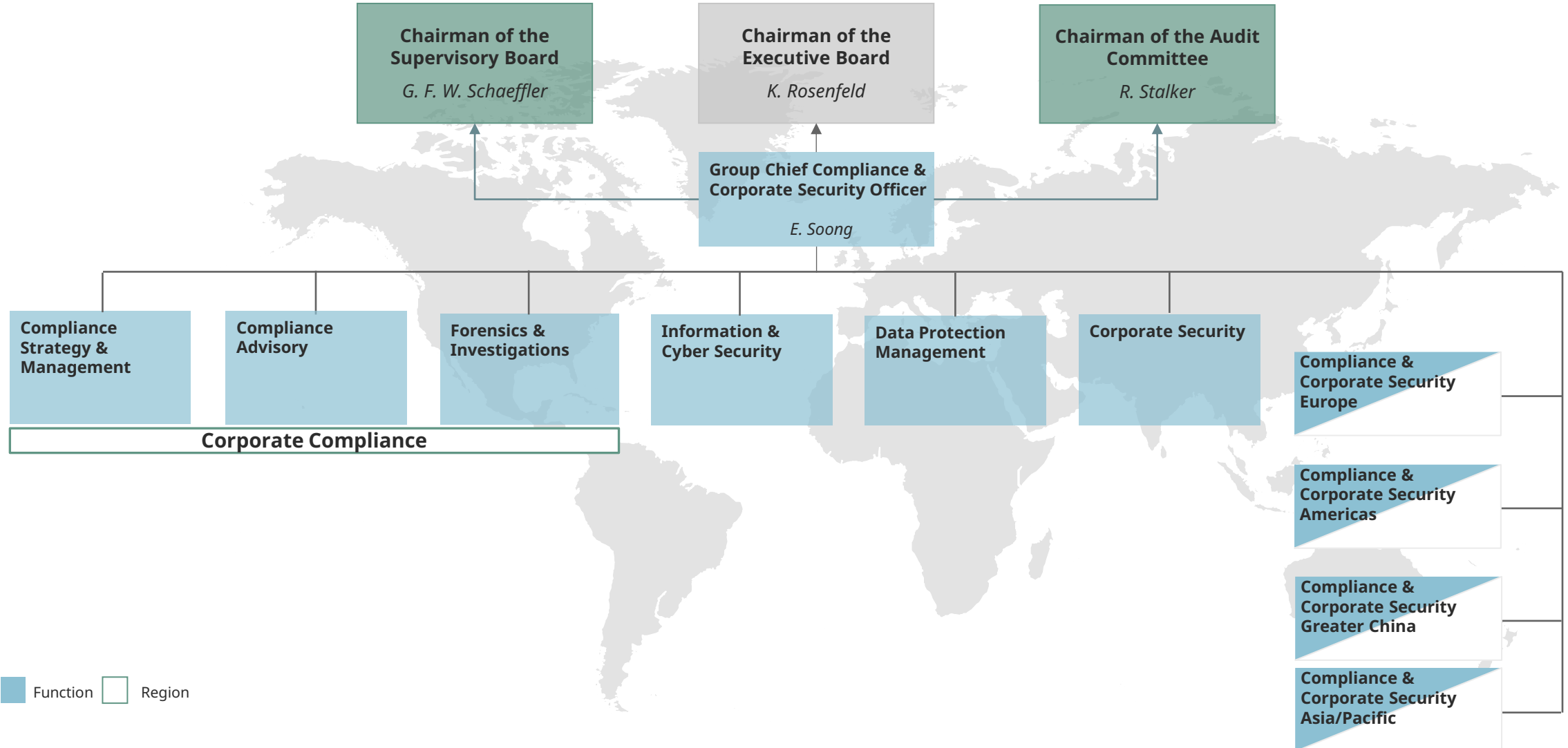
Neue Herausforderung: KI-Compliance

4

Ausrichtung an akzeptierten Industrie- und Prüfungsstandards

AGENDA

Governance Funktionen als „Independence Funktionen“



Compliance Management Systeme zur Handhabung aufkommender regulatorischer Vorgaben

2. TRENNUNG ALS EIGENSTÄNDIGE MANAGEMENT SYSTEME

Entwicklung eines integrierten Datenschutz Management Systems als **separates Compliance Management System** neben dem ISMS (u.a. aufgrund gesteigerter regulatorischer Anforderungen in beiden Bereichen, z.B. **NIS2**,...).



3. KI-COMPLIANCE UND EU AI ACT

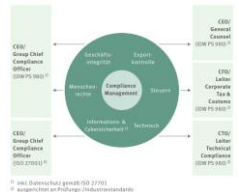
Compliance-Management Systematik für eine **vollumfängliche KI-Governance**.



1. INFORMATIONS- & CYBERSICHERHEIT INKL. DATENSCHUTZ

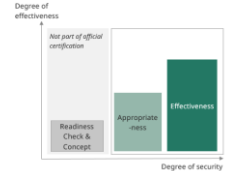
Informations- und Cybersicherheit zur Sicherung geistigen Eigentums und sensibler Daten (ausgerichtet an ISO/IEC 77001) und anderen relevanten Standards.

Datenschutz mit dem Fokus auf den Schutz von Persönlichkeitsrechten.

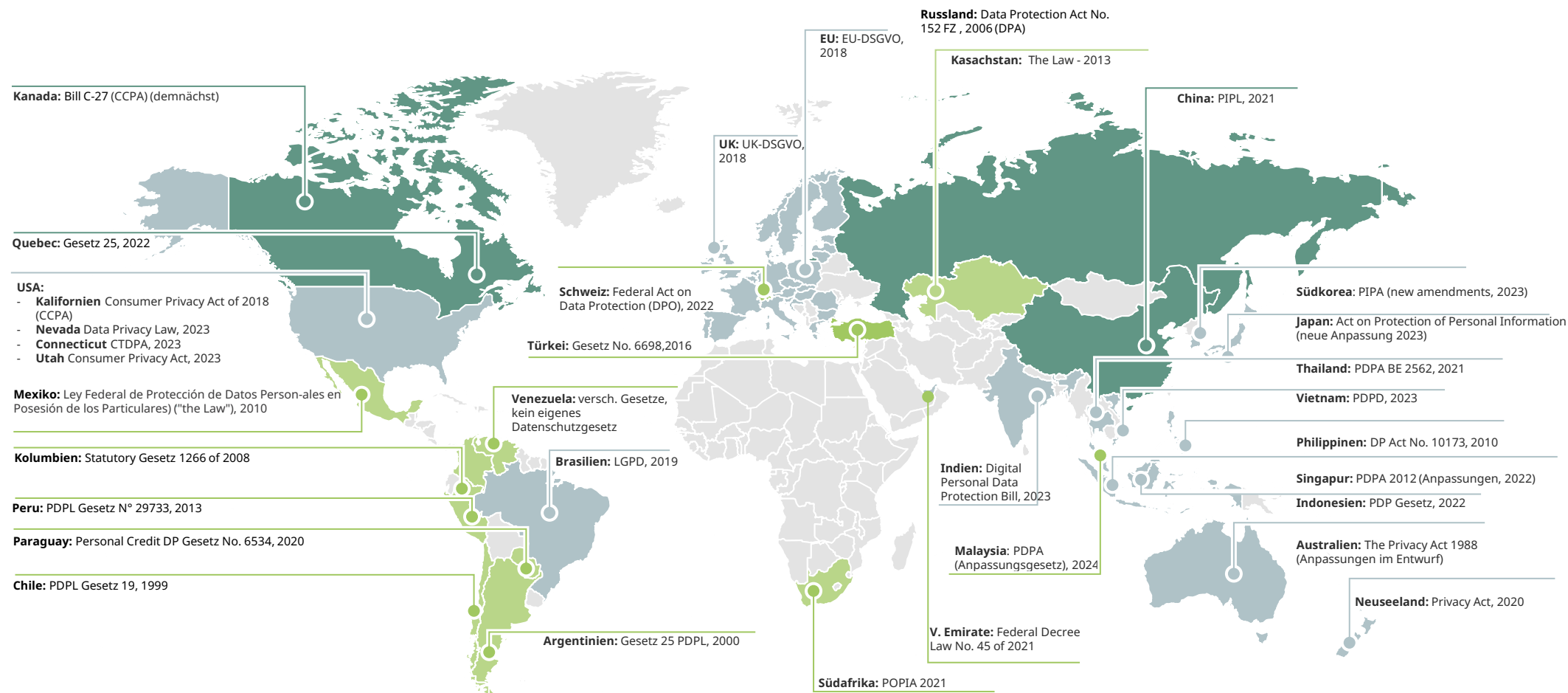


4. ZERTIFIZIERUNG

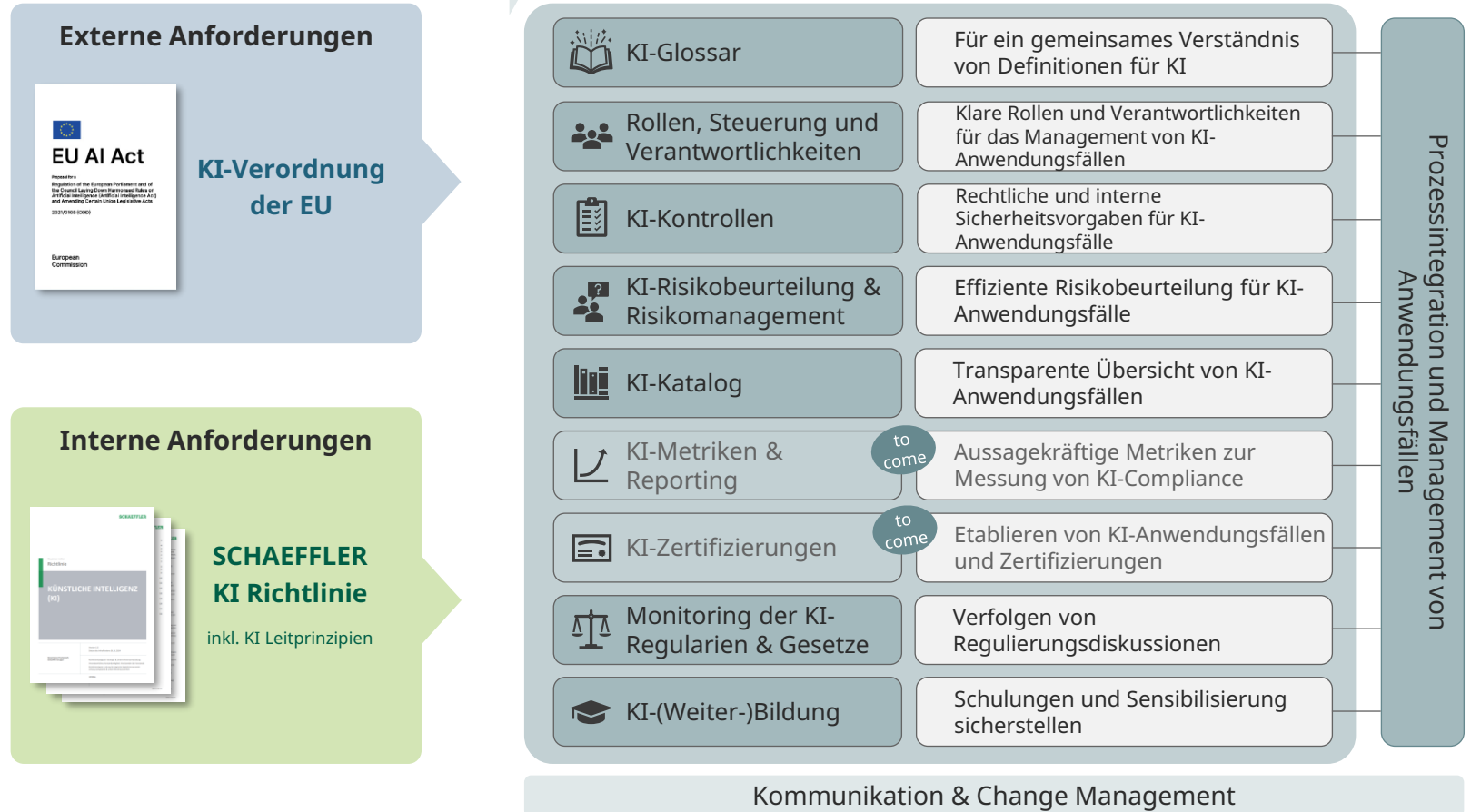
Nach Implementierung: **Zertifizierung** des Management Systems nach dem relevanten Prüfstandard z.B. **IDW PS 980**.



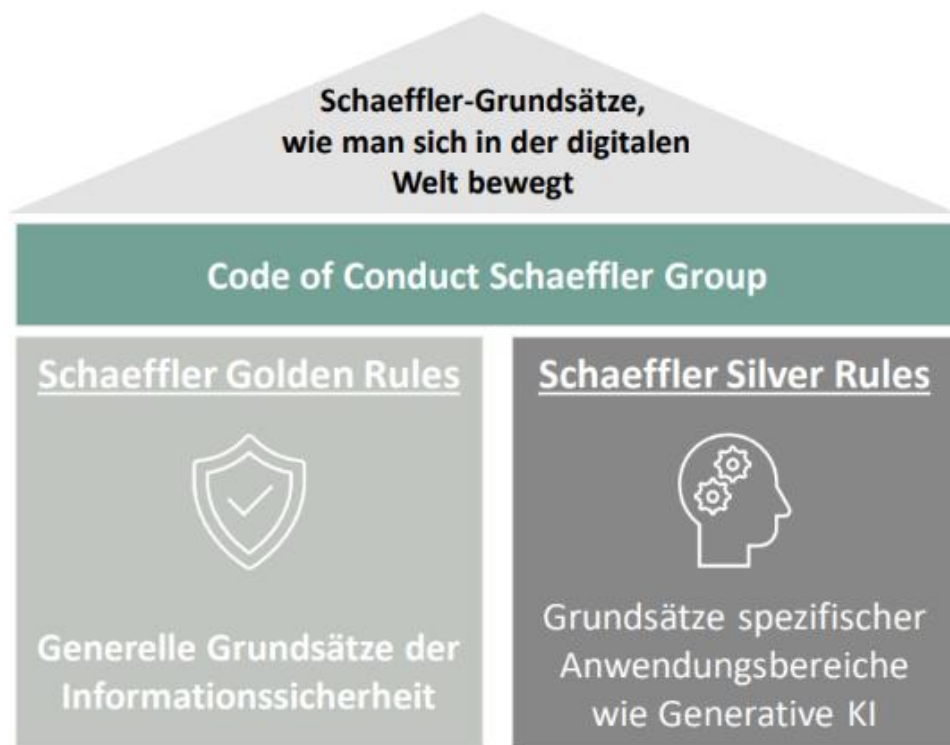
Zahlreiche datenschutzrechtliche regulatorische Anforderungen weltweit erfordern ein integriertes Datenschutz-Management-System



KI Compliance: “AI Operating Model” für eine vollumfängliche KI-Governance



„Silver & Golden Rules“ bei Schaeffler für den Einsatz Generativer KI



Schaeffler Silver Rules für Generative KI¹



Beachten Sie die allgemeinen Grundsätze der **Schaeffler Golden Rules**.



Verwenden Sie Generative AI nur mit **einer gesicherten Internetverbindung**.



Trainieren Sie die KI niemals **mit internen, vertraulichen oder persönlichen Informationen**. Alle Informationen, welche die KI erhält, müssen als öffentlich betrachtet werden. Seien Sie sich bewusst, dass Sie nicht wissen, wer diese Informationen sehen kann.¹



Lesen Sie **die Datenschutzrichtlinien** sowie die **Allgemeinen Geschäftsbedingungen** der jeweiligen Anwendung, um sich bewusst zu sein, wie Ihre Daten und die resultierenden Ergebnisse verwendet werden können.



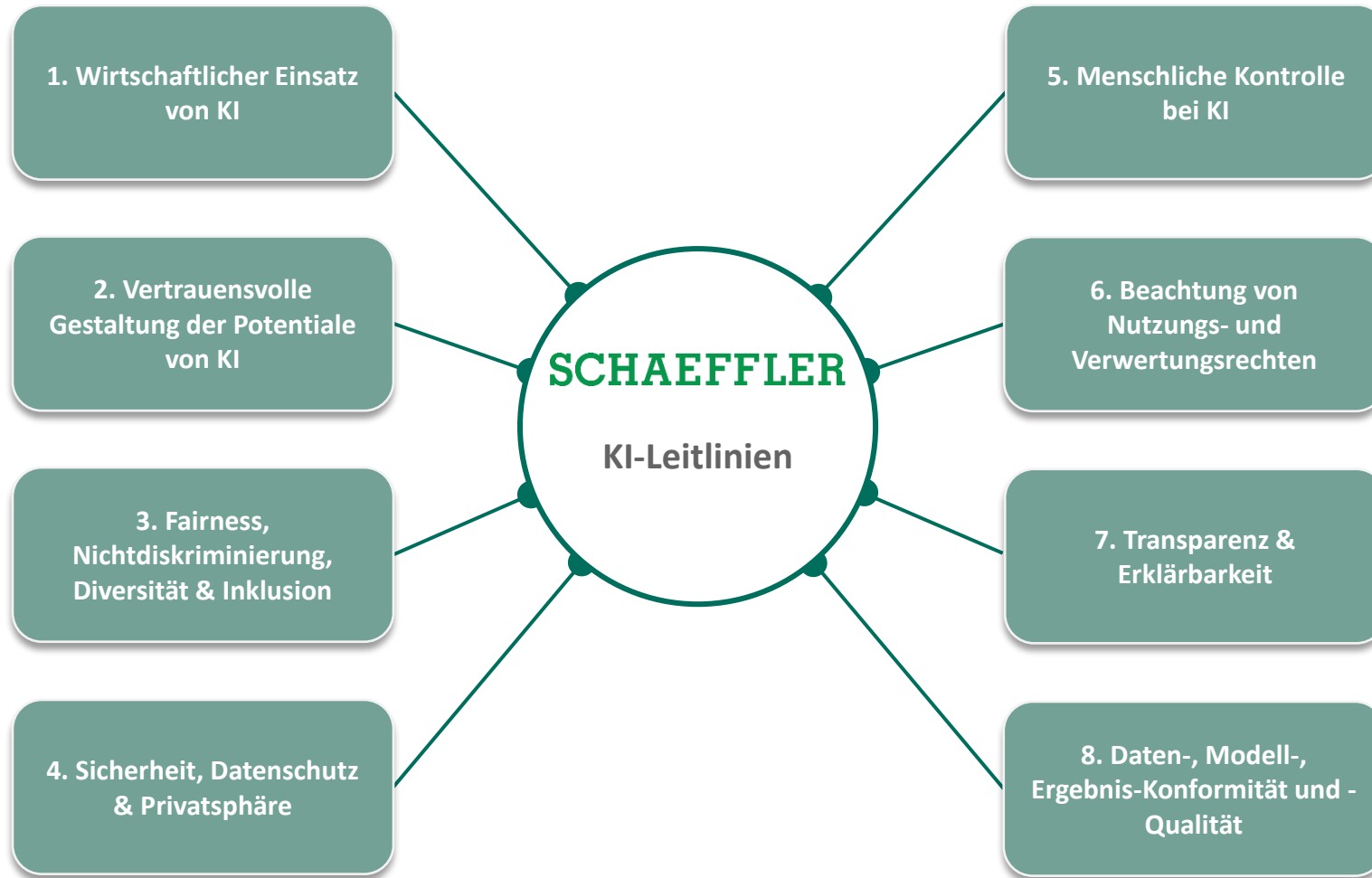
Anonymisieren Sie Daten beim Einsatz Generativer KI zum Schutz von Daten.¹



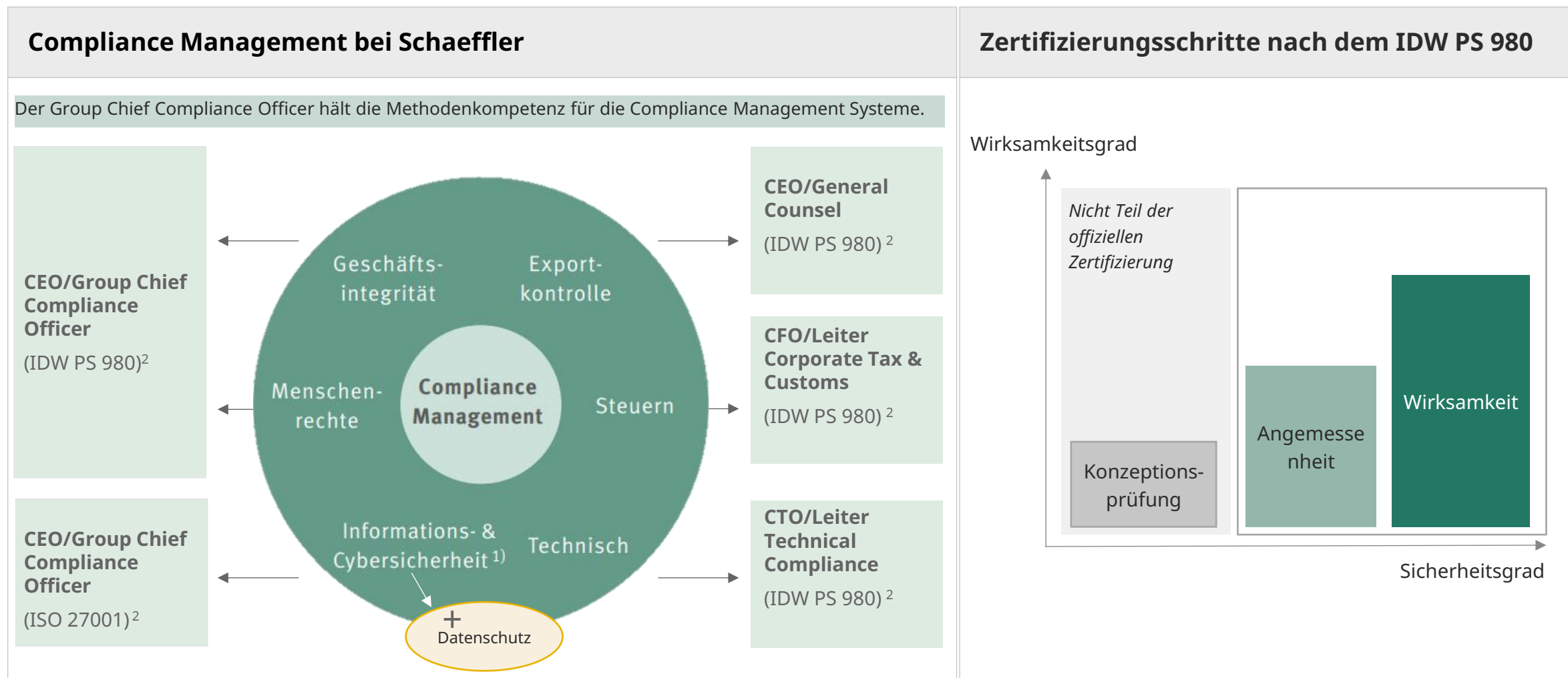
Vertrauen Sie nicht KI-Ergebnissen, ohne deren **Genauigkeit und Plausibilität zu verifizieren**. Der Bot stellt sein vermeintliches Wissen sehr überzeugend dar, aber **dies garantiert keine Korrektheit der Ergebnisse**. Zudem übernimmt der Bot keine Gewähr dafür, dass die Ergebnisse keine Rechte (einschließlich Copyrights) Dritter verletzen. **Kopieren und fügen Sie das Ergebnis nicht einfach nur ein**.

¹) Gültig für die Nutzung von öffentlichen Versionen von Generative AI, z.B. Dall-E, Bard. Für interne Versionen können die Regeln pro KI-Anwendung angepasst werden.

KI-Leitlinien und Vorgaben zur Umsetzung – 8 Prinzipien zu KI



Compliance Management Systeme bei Schaeffler - Sicherstellung eines konsistenten und an akzeptierten Industrie- und Prüfungsstandards ausgerichteten Vorgehens



¹ Inkl. Datenschutz gemäß ISO 27701.

² Ausgerichtet an Prüfungs-/Industriestandards.

SCHAEFFLER