IV. Entwicklung von Audit-Kontrollen

Wenn Sie Ihr Unternehmen auf die erste **interne oder externe Prüfung** vorbereiten, sollten Sie Kontrollen definieren, die ein Prüfer effizient und eindeutig nachprüfen kann. Wenn Sie einen Prüfer damit beauftragen, zu untersuchen, ob ein Unternehmen alle geltenden Gesetze oder Branchenstandards in Bezug auf KI einhält, muss der Prüfer ggf. unzählige Details, Ermessens- und Abwägungsentscheidungen untersuchen. Unter diesen Umständen können Sie kaum einen umsetzbaren oder aussagekräftigen Bericht erwarten. Daher sollten Sie in Erwägung ziehen, Prüfungskontrollen auf binäre Weise zu definieren, die mit „Ja- oder Nein"-Fragen überprüft werden können und die keinen Ermessensspielraum jenseits von Wesentlichkeitsschwellen zulassen oder erfordern. 11

Ein Prüfer kann zB effektiv überprüfen, ob ein Unternehmen: 12

- ein vollständiges Inventar der im Unternehmen eingesetzten KI unterhält,
- einen **menschlichen Systemverwalter (Administrator)** oder einen **Compliance Officer** benennt, der für jede KI verantwortlich ist,
- eine **schriftliche Folgen- und Risikobewertung** für jeden neuen KI-Einsatz dokumentiert und jährliche Aktualisierungen durchführt,
- Entwickler anweist, bei der Datenerfassung für das KI-Training die schriftlichen Leitlinien einzuhalten, und regelmäßig die Einhaltung bestätigt,
- **schriftliche Datenverarbeitungsverträge** mit allen externen KI-Anbietern hat, einschließlich der von der EU herausgegebenen Standardvertragsklauseln,
- Hinweise zur automatisierten Entscheidungsfindung ausgibt und allen betroffenen Personen ein Widerspruchsrecht anbietet,
- **Chatbots** offenlegt,
- bestätigt, dass alle Mitarbeiter eine jährliche Schulung zur Einhaltung der KI-Richtlinien absolvieren.

Unternehmensjuristen und Compliance-Beauftragte, die einige wenige binäre KI-bezogene **Audit-Kontrollen** zu den bestehenden Finanz-, Datenschutz- oder Informationssicherheits-Audit-Programmen eines Unternehmens hinzufügen, können Mitarbeitern und Management wiederholte und doppelte Befragungen ersparen sowie von den Ressourcen, Fähigkeiten und Methoden profitieren, die Auditoren zur Verfügung stellen. Nach der Durchführung von einigen Runden interner Audits sollten Unternehmen eine **externe Validierung ihres Compliance-Programms** durch professionelle Dritte in Betracht ziehen. Insbesondere Dienstleistungsunternehmen können besonders von unabhängigen Prüfberichten profitieren, um sich auf ihrem Markt zu profilieren und Bedenken potenzieller Kunden zu zerstreuen. 13

Kunden müssen die Relevanz und Aussagekraft der externen Prüfer und der in den Berichten verifizierten Kontrollen sorgfältig beurteilen können. In diesem Zusammenhang wurden Anbieter von **Datenschutz-„Siegeln"** und anderen Prüfberichten von Wirtschaftsverbänden kritisiert und sogar von Behörden wegen zu laxen Standards und irreführender Zertifizierungen sanktioniert. 14

Zitiervorschläge:
Determann KI-Recht/Determann §8 Rn. 11-14
Determann KI-Recht/Determann, 1. Aufl. 2025, §8 Rn. 11-14