Schmalenbach IMPULSE (2025) 5: 1-7
https://doi.org/10.54585/ MILZ5638

ESG-Governance – Voraussetzung für Compliance und effektive Steuerung von Nachhaltigkeit

Anne-Kathrin Gillig | Nadine-Lan Hönighaus *

1 Einleitung – vom Soft-Law zum Hard-Law

Das Akronym ESG – Environment, Social, Governance – beschreibt die drei zentralen Dimensionen nachhaltiger Unternehmensverantwortung. Erfasst werden ökologische Aspekte wie Klimaschutz und Ressourcenschonung, soziale Kriterien wie Arbeitsbedingungen und gesellschaftliches Engagement sowie Fragen einer verantwortungsvollen und ethischen Unternehmensführung, etwa im Hinblick auf Transparenz und Integrität.

ESG ist nicht lediglich eine Reaktion auf individuelle Erwartungen von Kunden, Verbrauchern oder Investoren, sondern Ausdruck eines umfassenden gesellschaftlichen Wandels und eine Antwort auf globale Herausforderungen. Der Klimawandel, der Verlust an Biodiversität, soziale Ungleichheit und die zunehmende Komplexität globaler Wertschöpfungsketten haben die Bedeutung nachhaltiger Unternehmensführung erheblich verstärkt. Der Global Risk Report 2025 unterstreicht diese Entwicklung eindrücklich: Klima- und Umweltrisiken zählen heute zu den größten Bedrohungen für globale Stabilität und wirtschaftliche Entwicklung.

Betrachtet man ESG im Licht der Carroll-Pyramide, so war nachhaltiges und verantwortungsbewusstes Handeln bislang vor allem Ausdruck ethischer und philanthropischer Unternehmensverantwortung – freiwillige Initiativen, die über gesetzliche Anforderungen hinausgingen. Mit der zunehmenden Kodifizierung von ESG-Standards auf nationaler und internationaler Ebene verändert sich jedoch diese Einordnung grundlegend: ESG wird zunehmend Teil der rechtlichen und wirtschaftlichen Verantwortung eines Unternehmens. Rechtlich bedeutet dies, dass Unternehmen gesetzlich verpflichtet sind, bestimmte ESG-Anforderungen – etwa im Be-

* Anne-Kathrin Gillig | Partnerin | KPMG Law Rechtsanwaltsgesellschaft mbH
Nadine-Lan Hönighaus | Partnerin | KPMG AG Wirtschaftsprüfungsgesellschaft

reich der Lieferkettensorgfalt, Klimaberichterstattung oder Governance-Standards – unter Androhung von Sanktionen und Haftungsrisiken verbindlich zu erfüllen.

Insbesondere auf europäischer Ebene nimmt die Dichte an Vorschriften kontinuierlich zu – daran hat auch die Omnibus-Initiative dem Grunde nach nichts geändert. Mit dem EU Green Deal als übergeordneter Strategie sind seit 2019 mehr als 179 neue Rechtsakte mit ESG-Bezug angestoßen und teilweise umgesetzt worden. Lediglich die drei bekannteren Regulierungsinstrumente, die Corporate Sustainability Reporting Directive (CSRD), die Corporate Sustainability Due Diligence Directive (CSDDD) und die EU-Taxonomie sind von der Omnibusinitiative betroffen, indem Inhalte und Pflichten vereinfacht wurden. Gänzlich abgeschafft sind auch diese Gesetze nicht und auch deren Vereinfachung ist zum Zeitpunkt der Veröffentlichung dieses Beitrags noch Gegenstand politischer Verhandlungen und Gesetzgebungsprozessen. Alle Regelungen zielen darauf ab, Menschenrechte und Nachhaltigkeit messbar, vergleichbar und rechtlich verbindlich in den Wertschöpfungsketten zu verankern. Gleichzeitig sorgen sie durch erhöhte Transparenz in der Berichterstattung dafür, dass Gesetzesverstöße schneller erkannt und verfolgt werden können.

2 Haftungsrisiken

Grundsätzlich obliegt der Unternehmensleitung eine Legalitätspflicht, also die Pflicht zur Rechtstreue. Dies bedeutet, dass sämtliche unternehmerische Entscheidungen und Maßnahmen im Einklang mit geltendem Recht und verbindlichen Normen stehen müssen. Ein Verstoß gegen gesetzliche Vorgaben ist daher nicht nur unzulässig, sondern kann weitreichende rechtliche Konsequenzen für die handelnden Organe nach sich ziehen.

Aus dem Legalitätsprinzip wird die sogenannte Legalitätskontrollpflicht abgeleitet. Diese verpflichtet die Geschäftsleitung dazu, angemessene Strukturen und Prozesse innerhalb des Unternehmens zu schaffen, um Gesetzesverstöße auf nachgelagerten Ebenen zu verhindern. Die konkrete Ausgestaltung dieser Kontrollmechanismen – also das „Wie“ – ist gesetzlich nicht abschließend geregelt. Vielmehr liegt es im unternehmerischen Ermessen, wie die Einhaltung rechtlicher Vorgaben organisatorisch sichergestellt wird. In der Praxis haben sich jedoch bestimmte Governance-Maßnahmen wie Compliance-Management-Systeme (CMS) etabliert.

Allen entsprechenden Systemen liegt dasselbe Ziel zugrunde: (rechtliche) Risiken zu minimieren und die Geschäftsleitung sowie das Aufsichtsgremium von (persönlicher) Haftung freizustellen. Zivilrechtlich besteht für Vorstandsmitglieder und Geschäftsführer die Gefahr, von der Gesellschaft auf Schadensersatz in Anspruch genommen zu werden, sofern sie ihre gesetzlichen oder gesellschaftsvertraglichen Pflichten verletzen. Solche Pflichtverletzungen können etwa darin bestehen, dass Rechtsverstöße nicht unterbunden wurden, wodurch der Gesellschaft finanzielle Schäden entstehen – beispielsweise durch entgangene Gewinne, behördliche Sanktionen, Kosten für Rechtsberatung oder interne Ermittlungen.

Auch strafrechtliche Risiken sind nicht zu unterschätzen. Mitglieder der Geschäftsleitung können strafrechtlich belangt werden, wenn sie gegen Schutzgesetze verstoßen oder es unterlassen haben, eine rechtlich gebotene Handlung vorzunehmen. Im ESG-Kontext gewinnen entsprechende Strafnormen zunehmend an Bedeutung: Unter dem Aspekt ökologischer Verantwortung können etwa Umweltstraftaten nach §§ 324, 330 StGB (z.B. Gewässerverunreinigung) einschlägig sein. Im sozialen Bereich treten insbesondere Verstöße gegen arbeitsrechtliche Vorschriften – wie illegale Arbeitnehmerüberlassung, Mindestlohnvergehen oder Schwarzarbeit – in den Vordergrund. In vielen Fällen resultiert die Verantwortlichkeit nicht aus aktivem Fehlverhalten, sondern aus Unterlassen, etwa dem Versäumnis, rechtlich gebotene Kontrollmaßnahmen einzuführen.

3 Wirksame ESG-Governance als Reaktion auf Regulierung

Im Zuge der zunehmenden ESG-Regulierung stehen Unternehmen vor der Aufgabe, ihre Governance-Strukturen kritisch zu hinterfragen und gezielt weiterzuentwickeln. Ausgangspunkt ist dabei die Frage, ob alle relevanten Rechtsvorschriften systematisch identifiziert wurden und alle maßgeblichen Stakeholder und deren Anforderungen angemessen berücksichtigt sind. Nur auf dieser Grundlage kann ein rechtssicheres und zugleich effizientes Steuerungssystem etabliert werden.

Im nächsten Schritt stellt sich die Frage, ob bereits bestehende Governance-Strukturen genutzt oder angepasst werden können, um die identifizierten ESG-Vorgaben wirksam umzusetzen. Eine bloße Formalerfüllung reicht dabei nicht aus. Vielmehr bedarf es einer systematischen Überprüfung und kontinuierlichen Weiterentwicklung der internen Strukturen, um regulatorische Anforderungen rechtzeitig zu erfüllen und operative Risiken zu minimieren.

Ein zentrales Element stellt hier die Relevanzanalyse dar. Unternehmen müssen zunächst prüfen, welche rechtlichen Vorgaben im Kontext von ESG – etwa im Rahmen des EU Green Deal – tatsächlich Anwendung auf ihr Geschäftsmodell finden.

Für die Bewertung der Relevanz kommen mehrere Kriterien in Betracht: Zum einen ist zu analysieren, ob und in welchem Umfang ein Gesetz oder eine Verordnung auf das Unternehmen zutrifft – abhängig etwa von Unternehmensgröße, Branche oder Tätigkeitsregion. Zum anderen sind zeitkritische Aspekte zu bewerten, also ob und wann die jeweilige Vorschrift in Kraft tritt und welcher Umsetzungsdruck daraus resultiert. Hinzu kommen potenzielle finanzielle Auswirkungen, wie Investitionen in neue Berichterstattungspflichten, Prozessanpassungen oder Lieferkettenmanagement. Schließlich ist das Risiko zu bewerten, das mit der Nichtbeachtung verbunden ist – etwa Bußgelder, Schadensersatzforderungen oder Reputationsverluste.

Ein praktikabler Bewertungsansatz ist die Anwendung eines Scoring-Modells, bei dem jede regulatorische Anforderung anhand festgelegter Kriterien – wie Anwendbarkeit, Dringlichkeit, wirtschaftlicher Auswirkungen

und Sanktionspotenzial – bewertet wird. Aus dem resultierenden Gesamtwert (Relevanzscore) lässt sich ableiten, welche regulatorischen Anforderungen prioritär zu behandeln sind. So entsteht eine strukturierte Shortlist relevanter ESG-Vorschriften, auf deren Basis konkrete Maßnahmen geplant und Ressourcen gezielt eingesetzt werden können.

4 Stakeholderanalyse im ESG-Kontext

In Ergänzung der Identifizierung und Bewertung der relevanten ESG-Rechtsvorschriften vervollständigt eine Stakeholderanalyse das Bild der maßgeblichen Rahmenbedingungen für ein wirksames ESG-Governance-Modell. Klassische Stakeholder eines Unternehmens haben ein Interesse an der Entwicklung und den Auswirkungen eines Unternehmens. Dazu zählen zum Beispiel Aktionäre, Mitarbeitende, Kunden, Lieferanten, Medien und Öffentlichkeit, Politik und Zivilgesellschaft, aber auch Umwelt und Natur als „stille Interessenträger“. Unternehmen bewegen sich nicht im luftleeren Raum, die Erwartungshaltung ihrer Stakeholder hat einen maßgeblichen Einfluss auf die „Licence to operate“ und damit die gesellschaftliche Wahrnehmung. Die balancierte Berücksichtigung von Stakeholder-Anforderungen ist für eine langfristig erfolgreiche Entwicklung des Geschäftsmodells und der Unternehmensstrategie entscheidend und sollte sowohl in die Unternehmensstrategie als auch in das Governance-Modell zur effektiven Umsetzung dieser Strategie Eingang finden. Die wachsende Bedeutung der Stakeholder und die Verpflichtung für Unternehmen, diese wirksam einzubeziehen, ist inzwischen rechtlich in der CSRD und auch der CSDDD verankert. Die CSRD legt beispielsweise fest, dass die Stakeholdersicht bei der Bestimmung der wesentlichen Auswirkungen, Risiken und Chancen durch ESG in der doppelten Wesentlichkeitsanalyse ermittelt werden muss und sowohl der Prozess als auch die Ergebnisse offengelegt werden sollen. Die CSDDD nennt Stakeholder-Dialog als ein zentrales Element der einzelnen Prozessschritte zur Umsetzung der unternehmerischen Sorgfaltspflichten.

Eine Stakeholderanalyse und ein anschließendes Stakeholdermapping bilden in Verbindung mit der rechtlichen Relevanzanalyse die Grundlage für die ESG-Strategie eines Unternehmens und das Ambitionslevel, für das ESG-Governance-Modell und ebenso für die ESG-Berichterstattung.

5 Weiterentwicklung der Governance-Systeme

Nach Identifizierung der relevanten Rechtsvorschriften sowie der Ermittlung der relevanten Stakeholder und ihrer Erwartungen kann nun eine Überprüfung erfolgen, ob die bestehenden Governance-Strukturen diese Anforderungen bereits hinreichend adressieren oder ob sie angepasst werden müssen. Ausgehend von dem Modell eines Compliance-Management-Systems (CMS) nach dem IDW PS 980, der sieben Elemente umfasst, können Rückschlüsse und Anpassungsbedarfe in folgender Form vorliegen:

- Compliance Kultur: Grundlage eines jeden CMS ist die Verankerung von Integrität und regelkonformem Verhalten in der Unternehmensführung und -kultur. Für ESG bedeutet dies, dass ökologische und soziale Werte nicht nur kommuniziert, sondern tatsächlich als „tone from the top“ vorgelebt werden – etwa durch eine öffentlich gelebte Null-Toleranz-Politik bei Umweltverstößen und Diskriminierung. Gleichzeitig könnte das Thema ESG prominent in den Code of Conduct aufgenommen werden.
- Compliance-Ziele: Grundsätzlich muss jedes CMS Ziele enthalten, die sich aus den unternehmensbezogenen Zielen ableiten und deshalb zu diesen nicht in Widerspruch stehen dürfen. Wenn als ESG-relevante Ziele beispielsweise die Reduktion von CO_2-Emissionen, die Einhaltung menschenrechtlicher Sorgfaltspflichten oder faire Vergütung entlang der Lieferkette genannt sind, so muss dies bspw. mit etwaigen Wachstumsstrategien des Unternehmens in Einklang gebracht werden.
- Compliance-Risikoanalyse: Ziel der Risikoanalyse innerhalb eines CMS ist es relevante Rechts- und Reputationsrisiken systematisch zu identifizieren und zu bewerten. Im ESG-Kontext sind dies z.B. Risiken im Bereich Umweltverschmutzung, Arbeitsbedingungen in der Lieferkette oder Risiken aus nichtfinanzieller Berichterstattung. Eine solche Risikoanalyse muss nicht nur regelmäßig, sondern auch bei Änderungen des geschäftlichen Umfelds, geänderten Produkten oder beispielsweise neuen Geschäftsbereichen des Unternehmens anlassbezogen durchgeführt werden.
- Compliance-Organisation: Für eine wirksame ESG-Governance ist eine klare organisatorische Verankerung innerhalb des Unternehmens unerlässlich. Soll die Unternehmensleitung wirksam von Haftungsrisiken entlastet werden, müssen Zuständigkeiten eindeutig definiert und Aufgaben ordnungsgemäß delegiert werden. Dies setzt voraus, dass die Geschäftsleitung die Verantwortung für ESG-Themen formal und inhaltlich an eine fachlich geeignete, organisatorisch klar zugeordnete Einheit überträgt. Darüber hinaus bedarf es abgestimmter ablauforganisatorischer Prozesse, die sicherstellen, dass die ESG-Organisation effektiv mit anderen Unternehmensbereichen – etwa Legal, Compliance oder Einkauf – zusammenarbeitet.

- Compliance-Programm: Grundsätzlich umfasst ein Compliance-Programm alle konkreten Maßnahmen, mit denen die definierten Ziele und die Vorgaben aus der Risikoanalyse praktisch umgesetzt werden. Im ESG-Kontext kann dies z.B. interne Richtlinien zum Lieferkettenmanagement, CO_2-Reduktionsprogramme, Verfahren zu Hinweisgebermeldungen oder ESG-spezifische Prüfprozesse betreffen. Entscheidend ist, dass das Programm nicht aus rein symbolischen Maßnahmen besteht, sondern strukturiert, dokumentiert und in der Praxis wirksam implementiert ist.
- Compliance-Kommunikation: Hierzu gehören Schulungen, Richtlinien und interne Kommunikation. Für ESG bedeutet dies u.a. regelmäßige Mitarbeiterschulungen zu Nachhaltigkeitsthemen und transparente Kommunikation über ESG-Ziele und -Maßnahmen.
- Compliance-Überwachung und -Verbesserung: Die Wirksamkeit eines jeden CMS muss regelmäßig überprüft und bei Bedarf angepasst werden. Die Aufgabe der Überwachung und Verbesserung eines Managementsystems wird traditionell von der internen Revision übernommen.

6 Bedeutung eines effektiven Legal Monitorings

Im Zuge der ESG-Governance-Diskussion gewinnt auch ein Thema zunehmend an Bedeutung: das effektive Legal Monitoring. Ausgehend von dem EU Green Deal antizipieren Unternehmen weitere Rechtsvorschriften, die Auswirkungen auf ihre Governance-Systeme haben können. Um rechtzeitig zu erkennen, welche Vorschriften für Unternehmen anwendbar sind und welche Auswirkungen solche Vorschriften auf die unternehmensinternen Governance-Systeme haben, sind Unternehmen gehalten, ein Monitoring aufzubauen, das die geltenden Rechtsvorschriften frühzeitig identifiziert.

Zunehmend setzen Unternehmen dabei auch auf den Einsatz digitaler Tools, um die Informationsflut effizient zu bewältigen. Automatisierte Monitoring-Systeme, intelligente Suchagenten und KI-gestützte Analyseplattformen ermöglichen es, relevante regulatorische Neuerungen schnell zu identifizieren, zu priorisieren und deren Auswirkungen strukturiert zu bewerten. Entscheidend bleibt jedoch, die technische Unterstützung durch eine enge menschliche Zusammenarbeit zu ergänzen: Nur im Dialog zwischen den Fachbereichen und der Rechtsabteilung kann gewährleistet werden, dass neue Anforderungen praxisgerecht interpretiert und wirksam umgesetzt werden.

7 Fazit und Ausblick

Ein wirksames ESG-Governance-System stellt sicher, dass rechtliche Anforderungen frühzeitig erkannt, strategisch bewertet und operativ umgesetzt werden. Dabei gilt es, bestehende Strukturen – insbesondere Compliance-Management-Systeme – gezielt weiterzuentwickeln, klare Verantwortlichkeiten zu schaffen, Prozesse zu verzahnen und durch ein effektives Legal Monitoring eine dauerhafte Rechtskonformität zu gewährleisten. Nur wenn ESG-Governance als integrierter Bestandteil von Unternehmensführung, Risikomanagement und Kultur verstanden wird, kann sie ihren Beitrag zur Wertschöpfung leisten und zugleich rechtliche sowie wirtschaftliche Risiken wirksam begrenzen. Auch die Omnibus-Initiative ändert nichts an der Wichtigkeit, die ESG-Themen in die Steuerungsinstrumente zu integrieren, da die Mehrzahl der ESG-Themen von dieser Initiative unangetastet bleibt.