Facility & Property Management als Trusted Data Provider -

auditierbare Daten durch gemeinsame Ökosysteme am Beispiel von Coalition-X

Whitepaper 2.0

GEFMA 984-6

Inhaltsverzeichnis

1. Vom ESG-Reporting zum vertrauenswürdigen Datenfluss: Ausgangslage, Zielsetzung und Bezug zu Coalition-X 4

1.1. Ausgangslage: ESG-Daten entstehen im Gebäudebetrieb....4

1.2. Zielsetzung: Vom Datenlieferanten zum Trusted Data Provider 5

1.3. Coalition-X als Orientierungsrahmen für vertrauenswürdige Datenflüsse....6

1.4. Gemeinsame Standards und digitale Vertrauensnachweise....8

1.5. Bedeutung für Property und Facility Management....9

2. Von operativen Rohdaten zum vertrauenswürdigen Datensatz: Datenprozesse und Kontrollmechanismen im PM und FM....9

2.1. Verantwortung im Datenprozess 9

2.2. Das interne Kontrollsystem (IKS) als Rahmen für verlässliche Daten....10

2.2.1. Grundelemente eines wirksamen Kontrollsystems 10

2.2.2. Risikobasierte Kontrollen und Stichproben 11

2.3. Anwendung entlang des Datenprozesses 11

2.4. Anwendung auf wesentliche Gebäudedaten 13

2.5. Verhältnismäßige Ausgestaltung bei kleineren Dienstleistern 17

2.6. Nutzen kontrollierter Datenprozesse für Dienstleister und Auftraggeber....17

3. Governance, Nachweisführung und Prüfung: Voraussetzungen für Vertrauen in ESG-Gebäudedaten 18

3.1. Governance und Verantwortungsverteilung entlang der Datenkette....18

3.1.1. Verantwortung für Erhebung, Verarbeitung, Freigabe und Weitergabe....18

3.1.2. Rollen und Verantwortungsgrenzen im Datenökosystem....20

3.1.3. Umgang mit Datenkonflikten und Korrekturen 20

3.2. Datenqualität als vertraglich definierte Leistung 21

3.3. Nachweisführung im Coalition-X-Ökosystem 21

3.3.1. Akkreditierung von Organisationen und Rollen....21

3.3.2. Datenmanagement und Kontrollprozesse....21

3.3.3. Credential und Unternehmenssiegel 22

3.3.4. Laufende Gültigkeit und Compliance....23

3.4. Von Vertrauensnachweisen zur unabhängigen Prüfung....24

3.5. Haftung und Umgang mit nachträglich erkannten Fehlern....25

4. Vom Datenlieferanten zum Trusted Data Provider - Handlungsbedarf und Ausblick....25

4.1. Gemeinsamer Handlungsbedarf entlang der Wertschöpfungskette....25

4.2. Ausblick: Datenökosysteme gemeinsam gestalten....28

1. Vom ESG-Reporting zum vertrauenswürdigen Datenfluss: Ausgangslage, Zielsetzung und Bezug zu Coalition-X

1.1. Ausgangslage: ESG-Daten entstehen im Gebäudebetrieb

Die Immobilienwirtschaft benötigt belastbare Daten zu Umwelt-, Sozial- und Governance-Aspekten (Environmental, Social and Governance, ESG) für Betrieb, Dekarbonisierung, Bewertung, Finanzierung und Berichterstattung. Entscheidend ist nicht allein deren Verfügbarkeit: Informationen müssen strukturiert, nachvollziehbar und auditierbar sein, um über Unternehmens- und Systemgrenzen hinweg genutzt werden zu können. Vertrauen in Daten entsteht dabei durch transparente Herkunft, dokumentierte Verarbeitung und klare Verantwortlichkeiten.

Das gefma-Whitepaper „ESG-Reporting im Property und Facility Management“ hat gezeigt: Belastbares ESG-Reporting beginnt im Gebäudebetrieb. Dort entstehen wesentliche Daten, die Eigentümer, Asset Manager, Investoren, Banken und Wirtschaftsprüfer benötigen – etwa zu Energie- und Wasserverbräuchen, Abfall, CO_2-Emissionen oder technischen Maßnahmen. Property Management (PM) und Facility Management (FM) sind damit zentrale Datenlieferanten der Immobilienwirtschaft.

Der Prozess dafür setzt sich aus 7 aufeinanderfolgenden Stufen zusammen. In Abbildung 1: *Elemente des ESG-Reporting-Prozesses* werden die unterschiedlichen Stufen aufgeführt in Verbindung mit den auszuführenden Beteiligten.

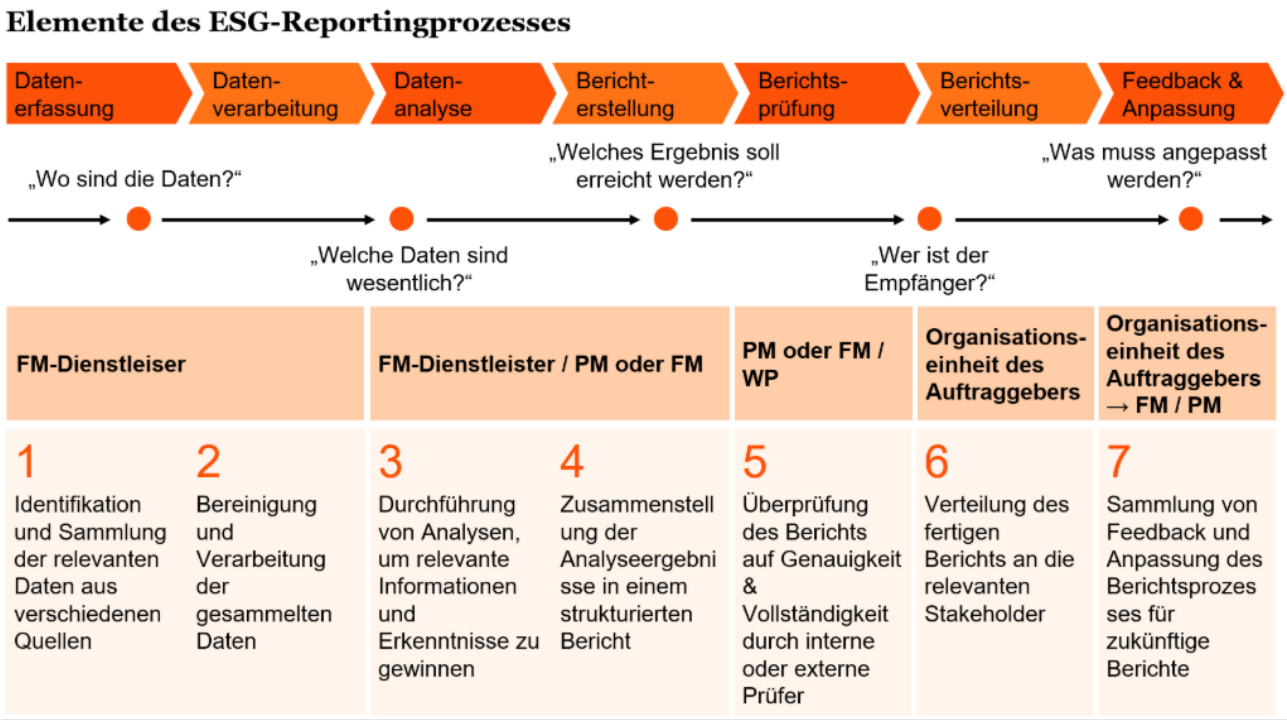


Abbildung 1: Elemente des ESG-Reporting-Prozesses, PwC

In der Praxis erschweren jedoch fragmentierte Systemlandschaften, uneinheitliche Definitionen und manuelle Übergaben die Nutzung dieser Informationen. Zugleich erhöht die zunehmende Vernetzung von Gebäudetechnik, IT-Systemen und Datenplattformen die Abhängigkeit von einer sicheren und verfügbaren digitalen Infrastruktur. Cyberangriffe, Systemausfälle oder Unterbrechungen in Dienstleisterketten können daher nicht nur den Gebäudebetrieb, sondern auch die Integrität und Verfügbarkeit berichtsrelevanter Daten beeinträchtigen.

Vertrauenswürdige ESG-Daten setzen deshalb neben fachlicher Datenqualität auch sichere und resiliente Datenprozesse voraus. Regulatorische Anforderungen wie NIS-2, die einschlägigen Regelungsrahmen für Betreiber kritischer Infrastrukturen (KRITIS), IT-Standards wie ISO/IEC 27001 oder Branchenstandards wie DORA für den Finanzsektor unterstreichen die Bedeutung eines systematischen Informationssicherheits- und Risikomanagements. Welche Anforderungen unmittelbar gelten, richtet sich nach dem jeweiligen gesetzlichen Anwendungsbereich. Über vertragliche Anforderungen und Lieferketten werden entsprechende Sicherheitsanforderungen jedoch auch für weitere PM- und FM-Dienstleister relevant.

1.2. Zielsetzung: Vom Datenlieferanten zum Trusted Data Provider

Dieses Whitepaper (2.0) knüpft an die im Whitepaper 1.0 erarbeiteten Grundlagen an und richtet den Blick auf den verlässlichen, standardisierten und prüffähigen ESG-Datenfluss aus Sicht von PM und FM, als Datenerzeuger, gegenüber dem Asset Management, Finanzierern, Eigentümern und Regulatoren als Datenempfänger. Die Kernbotschaft lautet: PM und FM müssen sich vom Data Provider zum Trusted Data Provider entwickeln. Ein Trusted Data Provider stellt Daten nicht nur bereit, sondern kann deren Herkunft, Verarbeitung, Qualitätssicherung und verantwortete Weitergabe nachvollziehbar nachweisen. Dafür muss der eigene Beitrag zur Datenkette von der Erhebung bis zur Weitergabe professionell gesteuert, abgesichert und dokumentiert werden.

Im Mittelpunkt stehen die dafür erforderlichen organisatorischen, prozessualen, technischen und vertraglichen Voraussetzungen: klare Verantwortlichkeiten, dokumentierte Datenprozesse, wirksame interne Kontrollen, sichere Schnittstellen sowie angepasste Verträge und Leistungsbilder. Für Datenempfänger hängt die Verwendbarkeit nicht nur vom Wert selbst, sondern auch von seiner nachvollziehbaren Entstehung ab. Für Kreditinstitute sind belastbare ESG-Informationen beispielsweise eine Grundlage für die Identifikation, Messung und Steuerung ESG-bezogener Risiken. Neben dem Datenwert gewinnen daher auch Herkunft, Aktualität, Verarbeitung und Qualität der zugrunde liegenden Gebäudedaten an Bedeutung.

Ein Trusted Data Provider muss darüber hinaus auch unter Störungen handlungsfähig bleiben. Resiliente Datenbestände müssen vor Verlust und unbemerkter Veränderung geschützt sowie aus gesicherten, nachvollziehbaren Datenständen wiederherstellbar sein. Resiliente Prozesse benötigen

definierte Ersatzverfahren, Eskalationswege und Wiederanlaufpläne. Resiliente (IT-)Organisationen erfordern klare Zuständigkeiten, qualifizierte Mitarbeitende, ein wirksames Vorfallmanagement und regelmäßig erprobte Notfallkonzepte. Dabei sind auch Abhängigkeiten von Plattformanbietern und weiteren Dienstleistern zu berücksichtigen.

Das Whitepaper zeigt, wie diese Anforderungen in die Erhebung, Verarbeitung, Kontrolle und Weitergabe von ESG-Gebäudedaten integriert werden können. Zugleich grenzt es die Verantwortlichkeiten von PM und FM gegenüber Auftraggebern, Plattformanbietern, Datenempfängern und Wirtschaftsprüfern ab. Professionell gesteuerte, abgesicherte und resiliente Datenprozesse schaffen die Voraussetzungen für automatisiertes ESG-Reporting, tragen zur Reduzierung von Prüf- und Haftungsrisiken bei und stärken das Vertrauen im Markt.

1.3. Coalition-X als Orientierungsrahmen für vertrauenswürdige Datenflüsse

Datenplattformen ermöglichen es, Informationen zusammenzuführen und für unterschiedliche Anwendungen und Zwecke bereitzustellen. Ihr organisationsübergreifender Nutzen entfaltet sich jedoch erst in einem interoperablen Daten*ökosystem*: durch gemeinsame Standards, überprüfbare Nachweise und verbindliche Regeln für einen sicheren Datenaustausch. Datenqualität, Datensouveränität und Resilienz müssen dabei über die Grenzen einzelner Organisationen hinaus betrachtet werden.

Dieses Whitepaper erläutert die damit verbundenen Anforderungen am Beispiel des derzeit entstehenden Datenökosystems Coalition-X. Gemeinsam mit verschiedenen Marktteilnehmern entwickelt das Projekt ein digitales Trust Framework für den standardisierten, gegen unbemerkte Veränderungen abgesicherten und nachvollziehbar dokumentierten Austausch von ESG-Gebäudedaten. Es soll Eigentümer, Investoren, Verwalter, Property und Facility Manager, Mieter, Wirtschaftsprüfer und Banken verbinden und die Nutzung der Daten auch für aufsichtsrechtliche und prüferische Zwecke unterstützen.

Ausgangspunkt der Initiative ist die Frage, warum die Datenkette entlang der Wertschöpfungskette – vom Ablesedienstleister über das Gebäudemanagement bis zum Kreditinstitut – immer wieder unterbrochen wird. An den Übergängen fehlen häufig einheitliche Qualitätsverfahren und maschinenlesbare Herkunftsnachweise. Prüf- und Plausibilisierungsaufwände verlagern sich dadurch auf nachgelagerte Empfänger, insbesondere Kreditinstitute, ohne dass ihnen die erforderlichen Informationen zur Datenentstehung und -verarbeitung vollständig vorliegen.

Coalition-X adressiert damit zwei zentrale Herausforderungen: Aufwand reduzieren und Risiken kontrollieren. Ziel ist ein marktneutrales Trust Framework für den verifizierbaren, souveränen und automatisierbaren Datenfluss – vom Gebäude bis zur Bank.

Abbildung 2 veranschaulicht, wie das Coalition-X Trust Framework die beteiligten Akteure entlang der Wertschöpfungskette verbindet und einen standardisierten, verifizierbaren Datenaustausch ermöglichen soll.

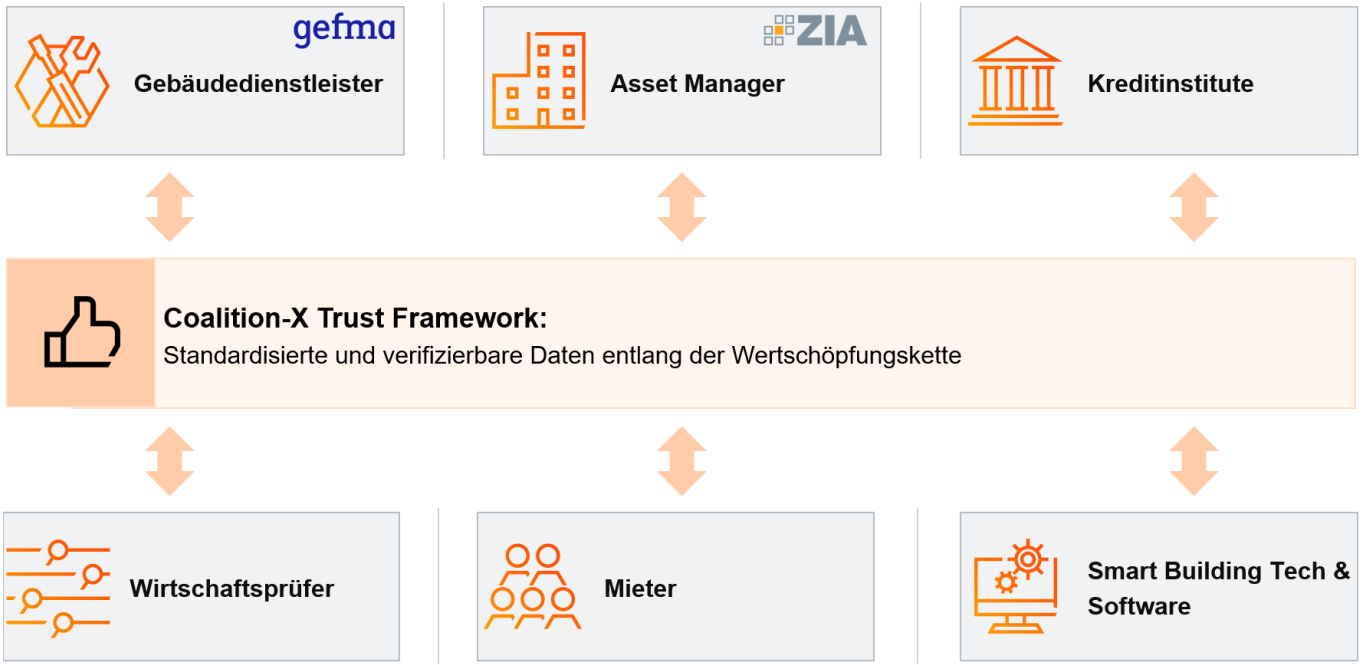


Abbildung 2: Coalition-X Trust Framework, Quelle: Coalition-X

Konnektoren und wiederverwendbare Nachweise sollen individuelle Schnittstellen, wiederholte Datenabfragen und redundante Prüfungen reduzieren. So können Daten effizienter für Finanzierung, Dokumentation, Reporting und die Steuerung der Immobilienbewirtschaftung genutzt werden. Die folgende Abbildung verdeutlicht, warum eine durchgängige Datenkette mit standardisierten Schnittstellen und nachvollziehbaren Nachweisen für die beteiligten Akteure erforderlich ist.

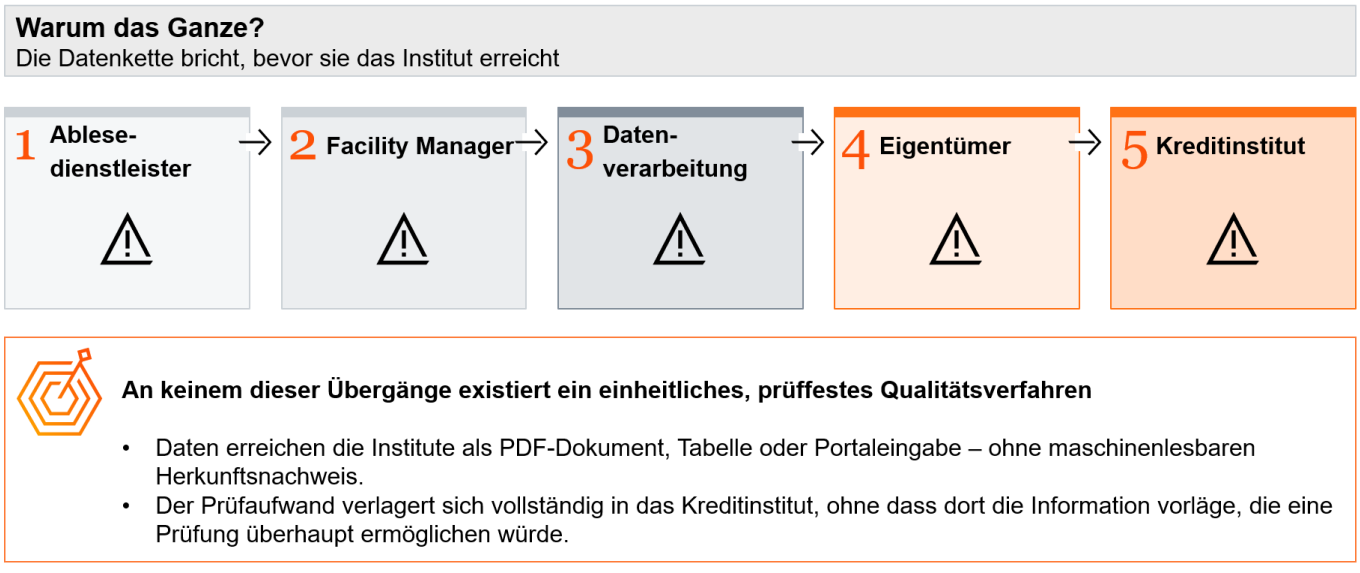


Abbildung 3: Die Datenkette, Quelle: Coalition-X

1.4. Gemeinsame Standards und digitale Vertrauensnachweise

Die fachliche Grundlage für die Standardisierung der Gebäudedaten bildet insbesondere die ZIA-Liste *Praktikable Nachhaltigkeits-KPIs für die Immobilienwirtschaft*. Ergänzend sind relevante Datenanforderungen aus regulatorischen und marktbezogenen Rahmenwerken zu berücksichtigen, etwa aus der EU-Taxonomie sowie aus Anforderungen der Finanzwirtschaft an ESG-bezogene Immobilieninformationen. Weitere fachliche Anknüpfungspunkte bilden die DIN SPEC 91475 Datenpunkte für die ökologische Analyse von Immobilien und das gefma-KPI-Tool (GEFMA 984-4; Bezug über gefma Shop).

Technologisch orientiert sich Coalition-X an den Prinzipien von Gaia-X und verfolgt eine offene, dezentrale und skalierbare Architektur. Bestehende Systeme und Datenplattformen sollen miteinander verbunden werden; die Datenhaltung verbleibt bei den jeweiligen Marktteilnehmern. Zugriffs- und Nutzungsrechte werden geregelt, ohne dass die jeweiligen Marktteilnehmer die Kontrolle über ihre eigenen Daten an eine zentrale Plattform abgeben.

Abbildung 4 veranschaulicht den Aufbau des Coalition-X Trust Frameworks. Die Governance-Ebene legt die gemeinsamen Regeln und Standards fest und überwacht deren Einhaltung. Die Trust-Ebene dient der Überprüfung von Identitäten, Berechtigungen und Datennachweisen. Die Exchange-Ebene ermöglicht den technischen Datenaustausch zwischen den beteiligten Systemen. Gemeinsam sollen diese Ebenen einen geregelten und nachvollziehbaren Datenaustausch ermöglichen.

Das Trust Framework umfasst drei Ebenen:



Abbildung 4: Das Trust-Framework, Quelle: Coalition-X

Maschinenlesbare Credentials bestätigen Identität, Rolle und Berechtigungen einer akkreditierten Organisation. Unternehmenssiegel ermöglichen es, die Herkunft und Integrität bereitgestellter Daten zu überprüfen und nachträgliche Veränderungen zu erkennen. Sie machen fachliche Kontrollen jedoch nicht überflüssig: Weder garantieren sie die inhaltliche Richtigkeit einzelner Werte noch ersetzen sie eine gegebenenfalls erforderliche unabhängige Prüfung.

1.5. Bedeutung für Property und Facility Management

Für PM und FM bietet Coalition-X einen Orientierungsrahmen für die Entwicklung vom reinen Datenlieferanten zum Trusted Data Provider. Organisationsübergreifende Vertrauensnachweise können dabei Transparenz über Herkunft und Integrität bereitgestellter Daten schaffen. Voraussetzung bleibt jedoch, dass die beteiligten Organisationen ihre eigenen Datenprozesse von der Erhebung bis zur Weitergabe professionell steuern, kontrollieren und dokumentieren.

Dazu gehören neben fachlicher Datenqualität auch sichere Schnittstellen, angemessene Berechtigungskonzepte, geschützte und wiederherstellbare Datenbestände sowie geeignete Notfall- und Wiederanlaufverfahren. Gesetzliche Anforderungen an Informationssicherheit und Resilienz sind entsprechend ihrem jeweiligen Anwendungsbereich unabhängig davon zu erfüllen. Die Teilnahme an einem Datenökosystem ersetzt weder das eigene Informationssicherheits- und Resilienzmanagement noch die fachliche Verantwortung für die bereitgestellten Daten.

Die folgenden Kapitel übertragen dieses Zielbild in die operative Realität von PM und FM. Sie zeigen, welche Anforderungen an Datenprozesse, interne Kontrollen, Governance, Nachweisführung sowie Sicherheit und Resilienz gestellt werden und wie daraus ein belastbarer, prüffähiger Datenfluss entlang der Immobilienwertschöpfung entstehen kann.

2. Von operativen Rohdaten zum vertrauenswürdigen Datensatz: Datenprozesse und Kontrollmechanismen im PM und FMVerantwortung im Datenprozess

Ein vertrauenswürdiger ESG-Datensatz entsteht nicht allein durch seine technische Übertragung oder Signierung. Voraussetzung ist vielmehr, dass für jeden Schritt des Datenprozesses klar geregelt ist, welche Organisation einen Datenpunkt originär erhebt oder aus einer bestehenden Quelle übernimmt, wer ihn verarbeitet und kontrolliert und wer ihn für die Weitergabe freigibt.

Im Property und Facility Management unterscheiden sich diese Verantwortlichkeiten je nach Datenart. Operative Verbrauchsdaten können unmittelbar durch das FM erhoben werden, etwa durch visuelle Zählerablesung, Smart Meter oder Gebäudeleittechnik. Andere Angaben werden aus bestehenden Primärquellen übernommen, beispielsweise aus Energieausweisen, Planunterlagen oder bereitgestellten

Bestandsdokumenten. Wieder andere Kennzahlen entstehen erst durch Konsolidierung, Berechnung oder fachliche Bewertung außerhalb des FM.

Entscheidend ist daher die Unterscheidung zwischen der Verantwortung für den Ursprungswert und der Verantwortung für dessen Übernahme und weitere Verarbeitung. Unabhängig davon, ob ein Wert originär erhoben oder aus einer externen Quelle übernommen wird, muss nachvollziehbar sein, woher er stammt, wie er verarbeitet wurde, welche Kontrollen durchgeführt wurden und welche Stelle ihn freigegeben hat.

2.2. Das interne Kontrollsystem (IKS) als Rahmen für verlässliche Daten

Im Regelfall erhebt oder verarbeitet ein FM-Dienstleister einen wesentlichen Teil der operativen Rohdaten, aus denen ESG-Kennzahlen entstehen. Seine Verantwortung richtet sich nach seiner konkreten Rolle im Datenprozess: Bei originär erhobenen Daten umfasst sie die kontrollierte Erfassung; bei übernommenen Daten die nachvollziehbare Quellenzuordnung und ordnungsgemäße Verarbeitung.

Ein IKS schafft hierfür den organisatorischen und prozessualen Rahmen. Es soll Risiken fehlerhafter, unvollständiger oder nicht nachvollziehbarer Datenverarbeitung angemessen adressieren und Abweichungen frühzeitig erkennen. Ein IKS begründet jedoch weder eine Garantie für die Richtigkeit jedes einzelnen Datenwerts noch automatisch Prüfungssicherheit.

2.2.1. Grundelemente eines wirksamen Kontrollsystems

Zentrale Grundlage ist eine nachvollziehbare Prozessdokumentation. Aus ihr sollte hervorgehen, wer welche Daten wann, aus welcher Quelle und gegebenenfalls mit welchem Mess- oder Erfassungssystem erhebt oder übernimmt.

Die Qualitätssicherung sollte grundsätzlich über automatisierte und datenpunktspezifische Plausibilitätsprüfungen erfolgen, etwa anhand von Pflichtfeldern, zulässigen Wertebereichen, Vorperioden, Einheiten sowie Objekt- und Zählerbezug.

Kontrollintensität und Freigabeanforderungen sollten sich am jeweiligen Risiko orientieren. Ein Vier-Augen-Prinzip ist nicht pauschal für jeden Datenpunkt erforderlich, sondern risikobasiert insbesondere bei wesentlichen manuellen Änderungen, begründeten Auffälligkeiten oder der Freigabe aggregierter Daten einzusetzen. Änderungen sind zu historisieren; Ursprungswerte dürfen nicht ohne nachvollziehbares Änderungsprotokoll überschrieben werden.

Ergänzend können risikobasierte Stichproben eingesetzt werden. Die Ausgestaltung der Kontrollen sollte sich an Datenart, Erfassungsmethode, Fehleranfälligkeit und Bedeutung des Datenpunkts orientieren.

2.2.2. Risikobasierte Kontrollen und Stichproben

Ein risikoorientiertes Kontrollsystem erfordert nicht zwingend eine Vollprüfung sämtlicher Datenpunkte. Abhängig von Art und Bedeutung der Daten sowie vom Kontrollziel können Stichproben eingesetzt werden. Dabei ist zwischen fachlicher bzw. risikoorientierter Auswahl und statistischen Stichprobenverfahren zu unterscheiden. Als methodische Orientierung können etablierte Normen herangezogen werden.

- DIN ISO 2859-1 für die Attributprüfung: Stichprobenpläne auf Basis eines akzeptablen Qualitätsgrenzwerts, übertragbar etwa auf die Frage, ob ein erfasster Zählerstand korrekt dokumentiert ist, geprüft über eine definierte Anzahl von Liegenschaften oder Belegen.

- DIN ISO 3951 für die Prüfung anhand quantitativer Merkmale, relevant, wenn nicht nur richtig oder falsch, sondern die Höhe einer Abweichung, etwa in Kilowattstunden, bewertet werden soll.

- DIN EN ISO 19011 als Leitfaden für Audits von Managementsystemen, mit Empfehlungen zur Stichprobenbildung bei Vor-Ort-Audits und Dokumentenprüfungen. Ein gut auf die Prüfung einzelner Objekte innerhalb eines Portfolios übertragbarer Ansatz.

Die konkrete Anwendbarkeit und Ausgestaltung eines Stichprobenverfahrens für ESG-Gebäudedaten ist daher anhand des jeweiligen Datenbestands, Kontrollziels und Risikoprofils festzulegen.

2.3. Anwendung entlang des Datenprozesses

Wie die Kontrollprinzipien in der Praxis ineinandergreifen, zeigt das in Tabelle 1 folgende Beispiel für Energiedaten. Entlang der Datenkette verändern sich sowohl die erforderlichen Kontrollhandlungen als auch die Verantwortlichkeiten. Fachliche Kontrolle, Freigabe, technische Siegelung und Weitergabe sind dabei als unterschiedliche Prozessschritte zu betrachten.

Schritt	Bezug zu Coalition-X
1**. Erfassung vor Ort auf Objektebene**: Ein Techniker liest den Zählerstand ab oder ein Smart Meter überträgt ihn automatisiert. Die IKS-Kontrollen erfolgen möglichst systemgestützt, etwa über Wertebereiche, Vorperioden, Objekt- und Zählerbezug sowie Zeitstempel. Bei manueller Erfassung kann ein Foto als Nachweis dienen. Ein Vier-Augen-Prinzip ist nur bei Auffälligkeiten oder risikobehafteten Korrekturen erforderlich, nicht bei jeder Ablesung.	Die IKS-Kontrolle und Protokollierung als Teil der Akkreditierungskriterien für Data Provider im Ökosystem
2. **Konsolidierung auf Portfolioebene**: Die Einzelwerte aller Liegenschaften werden im FM-System zusammengeführt. Kontrolliert wird über automatisierte Erkennung von Ausreißern und einen Abgleich hinsichtlich der Vollständigkeit, ob also alle Objekte gemeldet haben. Da nicht jedes Objekt einzeln vertieft geprüft werden kann, kommt hier eine Stichprobe zum Einsatz, etwa nach vereinbartem Qualitätsgrenzwert, eventuell basierend auf Ergebnissen aus zurückliegenden Reportingperioden.	Validierungsverantwortung und Protokollierung als Teil der Akkreditierungskriterien für Data Provider im Ökosystem
3**. Freigabe und Siegelung**: Der Dienstleister gibt den definierten Datenbestand nach festgelegten Kontrollen frei. Die Freigabe muss nicht für jeden einzelnen Datenpunkt manuell erfolgen. Nach erfolgreicher Prüfung kann die Siegelung systemseitig automatisiert ausgelöst werden; manuelle Freigaben sind nur für Ausnahmen, Korrekturen oder festgelegte Berichtsstände vorgesehen.	Automatisierte Siegelung der freigegebenen Daten mit dem gültigen Coalition-X-Credential; fachliche Freigabe und technische Siegelung bleiben getrennte Schritte.
4. **Übergabe an das Drittsystem des Auftraggebers**: Etwa ein ESG-Reporting-Tool oder ERP-System: Hier greift eine Schnittstellenkontrolle, die die Datenintegrität bei der Übertragung sicherstellt und manuelle Nachbearbeitung ohne Protokoll ausschließt. Die Verantwortung des FM-Dienstleisters endet an der vertraglich und technisch definierten Übergabestelle; Kontrollen in nachgelagerten Systemen liegen bei der jeweils verantwortlichen Organisation.	Geregelte und geschützte Übertragung über den Exchange Layer bzw. einen standardisierten Konnektor; die Verantwortung ist je Übertragungsabschnitt abzugrenzen.

Tabelle 1: Praxisbeispiel - Energiedaten vom Zähler bis zum Drittsystem

So entsteht eine dokumentierte und nachvollziehbare Kette von den einzelnen Messwerten bis zur konsolidierten Kennzahl im Bericht des Auftraggebers. Sie kann eine Grundlage dafür bilden, dass interne und externe Adressaten Herkunft, Verarbeitung und Kontrollschritte des Datenpunkts beurteilen können. Coalition-X unterstützt die Freigabe und Übergabe in den Schritten 3 und 4 durch maschinenlesbare Herkunftsnachweise auf Basis nachgewiesener IKS-Prozesse sowie eine sichere und skalierbare Übertragungsmöglichkeit.

Die Nachweiskette kann anschließend über weitere Organisationen fortgeführt werden: Beispielsweise übernimmt das PM die gesiegelten FM-Daten und ergänzt eigene Angaben; das Asset Management führt diese mit weiteren Beiträgen zu einem Objekt- oder Portfoliodatensatz zusammen. Die jeweils verantwortete Bereitstellung oder Zusammenstellung wird mit einem eigenen Unternehmenssiegel

versehen, während die Nachweise der Vorstufen erhalten und zugeordnet bleiben. Der abschließende Datenempfänger kann die verknüpften Nachweise prüfen und etwaige Rückfragen gezielt, an die für den jeweiligen Beitrag verantwortliche Organisation richten. Dadurch können die Aufwände bei Nachprüfungen reduziert werden.

2.4. Anwendung auf wesentliche Gebäudedaten

Die dargestellten Kontrollprinzipien entfalten ihre Wirkung erst durch ihre konkrete Anwendung auf einzelne Datenarten. Welche Kontrollhandlungen erforderlich und angemessen sind, hängt insbesondere davon ab, aus welcher Quelle ein Datenpunkt stammt, wie er erhoben oder übernommen wird, welche Verarbeitungsschritte erfolgen und welche Rolle Property Management oder Facility Management dabei übernimmt. Nicht jeder Datenpunkt erfordert daher dieselben Kontrollhandlungen oder dieselbe Kontrollintensität.

Die folgende tabellarische Übersicht überträgt die Kontrollprinzipien auf die im Coalition-X-Kontext betrachteten ESG-Gebäudedaten. Sie unterscheidet, ob das FM einen Datenpunkt originär erhebt, aus einer Primärquelle übernimmt, fachlich plausibilisiert, konsolidiert oder lediglich für die Weitergabe bereitstellt. Zugleich werden typische Nachweise und wesentliche Verantwortungsgrenzen dargestellt.

Die Übersicht beschreibt keine eigenständigen Coalition-X-Akkreditierungskriterien und begründet keine automatische Prüfungssicherheit. Die datenliefernde Organisation bleibt für einen beherrschten Datenprozess verantwortlich; die Tabelle konkretisiert hierfür aus PM- und FM-Sicht typische Quellen, Kontrollen, Nachweise und Verantwortungsgrenzen. Die Kontrolle von Vollständigkeit und Richtigkeit ist dabei weder als Garantie der Fehlerfreiheit noch als lückenlose manuelle Einzelprüfung jedes Datenpunkts zu verstehen, sondern als dokumentierte, datenpunktspezifische und risikoorientierte Plausibilisierung. Die folgende tabellarische Übersicht konkretisiert diese Grundsätze anhand der im Coalition-X-Kontext betrachteten Datenpunkte der ZIA-KPI-Liste.

Datenart	Daten-beispiel	Quelle	Erfas-sungsart	Nachweis	Methode zur prüfsicheren Erhebung	Erwartung des Wirtschaftsprüfers
Cluster 1 – Objekt Stammdaten (ZIA-KPI 1-2)						
Objekt-ID	Eindeutige Objekt-kennung	CAFM-System	Digital	System-eintrag	Stabile, eindeutige ID im System des Datenlieferanten; Änderungen und Statuswechsel werden protokolliert, keine Wiederverwendung freigewordener IDs (bei Objektabgang entsteht ein Statuswechsel mit Archivierung, statt Löschung) .	Eindeutige und richtige Zuordnung; jedes berichtspflichtige Objekt genau einmal angelegt; keine Doppelanlagen, keine Lücken im Bestand.
Gebäude-adresse / Geoko-ordinaten	Adresse	CAFM / ERP Grundbuch	Digital / manuell	System-eintrag	Übernahme aus Primärquelle, Abgleich mit Grundbuchangaben bei Ersterfassung, Plausibilitätsprüfung der Koordinaten inkl. Dokumentation	Konsistenz (auch über Berichtsperioden stabil)
Nutzungs-art / Mixed-Use-Anteile	Wohnen, Büro, Handel, etc. inkl. Flächen-anteile	Mietver-trag, andere externe Quellen	Manuell	Vertrags-unterlage	Nutzungsart und Flächenanteile werden aus festgelegter Quelle übernommen. Quelle, Stand und verwendete Flächendefinition werden dokumentiert. Anteile werden auf Vollständigkeit und eine plausible Gesamtsumme geprüft.	Dokumentierter Ursprung (einheitliche Klassifikation, Flächenanteile vollständig und summengeprüft)
Baujahr	Jahreszahl	Bauakte	Manuell	Bauunter-lagen	Direkte Übernahme aus festgelegter Primärquelle mit Quellenverweis und Dokumentversion. Bei widersprüchlichen Angaben gilt eine dokumentierte Quellenpriorität; ungeklärte Werte werden gekennzeichnet.	Nachweis vorhanden (Baujahr stimmt mit Nachweisdokument überein und bestätigt Richtigkeit)
Cluster 2 – Energieausweis / EPC (ZIA-KPI 3)						
Ausweis-typ	Bedarfs- oder Ver-brauchs-ausweis	Energie-ausweis-Dokument	Manuell	Ausweis-dokument	Direkte Übernahme aus dem Originaldokument oder einer maschinenlesbaren Kontrolldatei. Pflichtfeld- und Zulässigkeitsprüfung verhindert die Vermengung von Bedarfs- und Verbrauchsausweis; Gültigkeit wird mitgeführt.	Eindeutige Typzuordnung

Daten art	Daten-beispiel	Quelle	Erfassungs-art	Nachweis	Methode zur prüfsicheren Erhebung	Erwartung des Wirtschaftsprüfers
Energie-effizienz-klasse	A+ bis H	Energie-ausweis	Manuell	Ausweis-dokument	Direkte Übernahme aus dem Originaldokument (bzw. der XML-Kotrolldatei, falls vorhanden) inkl. Ausweis-gültigkeit, hinterlegt im CAFM-System. Hinweis: Coalition-X implementiert die Fraunhofer-Methodik zur automatisierten Klassifizierung der Nichtwohngebäude, sodass ein maschinenlesbarer Wert direkt signiert übernommen werden kann.	Nachweis vorhanden (Energieeffizienzklasse stimmt mit Nachweisdokument überein und bestätigt Richtigkeit)
Primär-energie-bedarf	kWh/m²a	Energie-ausweis, Energie-berater	Manuell	Ausweis-dokument	Direkte Übernahme aus dem Originaldokument (bzw. der XML-Kotrolldatei, falls vorhanden), das bedeutet eine Übernahme ohne Kontrollschritt Hinweis: Coalition-X erzeugt aus der xml-Kontrolldatei einen maschinenlesbaren Wert, der direkt signiert übernommen werden kann.	Nachvollziehbarer Ursprung durch Quellen- und Erfassungskontrolle
Ausstel-lungsda-tum / Gültigkeit	Datum, Ablauf nach 10 Jahren	Energie-ausweis	Manuell	Ausweis-dokument	Direkte Übernahme der Datumsangaben aus dem Energieausweis; automatische Fristprüfung und Kennzeichnung abgelaufener oder zeitnah auslaufender Dokumente. Verantwortlichkeit und Reaktionsfrist für die Klärung sind definiert.	Aktualität sichergestellt (abgelaufene Ausweise erkannt und gekennzeichnet)
Cluster 3 – Energieverbrauch & -mix (ZIA-KPI 4–5)						
Stromver-brauch	kWh/a je Zähler	Smart Meter, EVU-Rechnung	Digital / Visuell	Messwert, Rechnung	Automatische Übertragung ohne Medienbruch, Zeitstempel, Historisierung, Abgleich Rechnung zu Messwert. Bei manueller Ablesung Fotodokumentation mit Zeitstempel und (qualifiziertem) Erfasser, dokumentierte Stichprobe (z.B. Test der automatischen Messwerte), vollständiges	Nachvollziehbare Messkette, vollständiger Zählerbezug und dokumentierte Plausibilisierung; Eich- und Wechselinformationen werden berücksichtigt, soweit relevant und verfügbar

Datenart	Datenbeispiel	Quelle	Erfassungsart	Nachweis	Methode zur prüfsicheren Erhebung	Erwartung des Wirtschaftsprüfers
					Zählerverzeichnis je Objekt inkl. Zählerkarten, Monitoring der Eichfristen, Abgleich bei Zählerwechsel und systemische Dokumentation des Wechsels.	
Wärmeverbrauch	kWh/a, Wärmemenge	Wärmezähler, Fernwärmerechnung	Digital / Visuell	Messwert, Rechnung	Fernauslesung wird bevorzugt. Bei manueller Ablesung werden Zeitstempel, Objekt- und Zählerbezug sowie Foto- oder vergleichbarer Beleg dokumentiert. Plausibilisierung erfolgt anhand geeigneter Vorperioden, erneute Ablesung nur bei begründeter Auffälligkeit; Stichprobenumfang risikobasiert.	Nachweis der Ablesung durch Foto mit Zeitstempel, geeichte Zähler (nachgewiesen) + Überwachung der Eichfristen
Kälteverbrauch	kWh/a	GLT, Energiemanagementsystem	Digital	Trenddaten	Automatisierte Übernahme aus GLT oder Energiemanagementsystem mit Zeitstempel, Objekt- und Messpunktbezug sowie Historisierung. Plausibilisierung anhand von Datenlücken, zulässigen Wertebereichen und geeigneten Vorperioden; Berechnungsregeln und Änderungen sind versioniert.	Auditierbare Rohdaten
Energieträgeranteile	z. B. Erdgas / Fernwärme / Strom in %	Abrechnungen, Verbrauchsdatenaggregation	Digital / Visuell	Rechnung, Systemauswertung	Zuordnung je Energieträger im ESG-Tool; Plausibilitätsabgleich: Summe der Anteile (inkl. Abgleich Zuordnung je Energieträger) = Gesamtverbrauch	Konsistente und richtige Aufteilung (Zuordnung je Energieträger nachweisbar richtig)
Anteil erneuerbare Energien	% Endenergie, ggf. PV-Eigenerzeugung	EVU-Herkunftsnachweis, PV-Zähler	Digital / Visuell	Herkunftsnachweis, Messwert	Nicht im Fokus vom FM. Falls beauftragt: Anteil aus Netzbezug anhand geeigneter Herkunftsnachweise übernehmen; PV-Eigenerzeugung separat und messwertbasiert erfassen. Prüfung zusätzlicher Qualitäts- oder Additionalitätskriterien nur bei ausdrücklicher Anforderung.	Belastbarer Anteilsnachweis (durch externe Quelle bestätigt)

Tabelle 2: Datenarten, typische Quellen und Methodendarstellung zur prüfsicheren Erhebung im Rahmen von Coalition-X / der ZIA-KPI-Liste

2.5. Verhältnismäßige Ausgestaltung bei kleineren Dienstleistern

Für FM-Dienstleister, die aus wirtschaftlichen oder organisatorischen Gründen über kein formalisiertes internes Kontrollsystem (IKS) verfügen, kann alternativ ein vereinfachtes, dokumentiertes Qualitätssicherungs- und Kontrollverfahren eingesetzt werden. Dieses muss nicht zwingend auf einer spezialisierten Softwarelösung basieren, sondern kann beispielsweise durch standardisierte digitale Erfassungsformulare, strukturierte Excel-Tabellen oder einfache FM-Systeme umgesetzt werden.

Entscheidend ist, dass die Herkunft der ESG-Daten, der Erfassungszeitpunkt, die verantwortliche Person sowie vorgenommene Änderungen und Plausibilitätsprüfungen nachvollziehbar dokumentiert werden. Die Qualitätssicherung kann durch definierte Prüfroutinen, Vorperiodenvergleiche, Zählerfotos und risikobasierte Stichproben erfolgen.

Bei wesentlichen Abweichungen oder nachträglichen Korrekturen ist eine zusätzliche Kontrolle vorzusehen. Umfang und Ausgestaltung des Kontrollsystems sollten dabei den Risiken, der Komplexität der Datenprozesse und dem Umfang der bereitgestellten Daten angemessen sein. Ob die dokumentierten Kontrollen für eine externe Prüfung oder eine Akkreditierung im jeweiligen Datenökosystem ausreichen, ist anhand der jeweiligen Anforderungen gesondert zu beurteilen.

2.6. Nutzen kontrollierter Datenprozesse für Dienstleister und Auftraggeber

Für den Dienstleister sind dokumentierte und wirksame Kontrollverfahren zunächst ein Qualitätsargument gegenüber berichtspflichtigen Auftraggebern. Ein methodisch stringenter Prozess kann Rückfragen und Ad-hoc-Erklärungen im Prüfungsprozess reduzieren, die Nachweisfähigkeit gegenüber Auftraggebern verbessern und dazu beitragen, Fehler und damit verbundene Haftungsrisiken frühzeitig zu erkennen. Zugleich stärkt ein nachvollziehbar kontrollierter Datenprozess die Position des Dienstleisters als verlässliche Datenquelle innerhalb der Datenkette.

Auch für den Auftraggeber schaffen solche Kontrollverfahren einen Mehrwert. Belastbare Kontrollen beim Datenlieferanten verbessern die Nachvollziehbarkeit der bereitgestellten Daten und können Rückfragen sowie zusätzliche Datenaufbereitungen reduzieren.

Darüber hinaus kann die nachvollziehbare Dokumentation der Kontrollverfahren die Verwertbarkeit vorhandener Kontrollen erhöhen und Prüfungsaufwände reduzieren. Ob und in welchem Umfang ein Wirtschaftsprüfer auf vorhandene Kontrollen und Nachweise zurückgreifen kann, hängt jedoch vom jeweiligen Prüfungsgegenstand sowie von seiner Beurteilung der Ausgestaltung und Wirksamkeit der Kontrollen ab.

Insbesondere bei großen Immobilienportfolien können risikoorientierte und, soweit methodisch geeignet, stichprobenbasierte Kontrollverfahren dazu beitragen, Kontrollaufwände effizient auszurichten. Voraussetzung ist, dass Auswahlverfahren, Kontrollhandlungen, Ergebnisse und Abweichungen nachvollziehbar dokumentiert werden.

3. Governance, Nachweisführung und Prüfung: Voraussetzungen für Vertrauen in ESG-Gebäudedaten

3.1. Governance und Verantwortungsverteilung entlang der Datenkette

3.1.1. Verantwortung für Erhebung, Verarbeitung, Freigabe und Weitergabe

Kapitel 2 beschreibt, wie ESG-Gebäudedaten erhoben, verarbeitet, kontrolliert und weitergegeben werden. Damit diese Prozesse Vertrauen schaffen, muss zugleich eindeutig geregelt sein, welche Organisation welchen Beitrag zur Datenkette verantwortet und wer innerhalb dieser Organisation die jeweiligen Aufgaben übernimmt.

Dabei sind zwei Ebenen zu unterscheiden: Nach außen muss erkennbar sein, welche Organisation für einen Datenbeitrag verantwortlich ist. Innerhalb der Organisation müssen die Aufgaben und Befugnisse für Erhebung, Verarbeitung, Kontrolle, Freigabe und Weitergabe konkret zugewiesen sein. Werden operative Aufgaben an Dritte übertragen, sind auch deren Zuständigkeiten und die Verantwortungsgrenzen eindeutig festzulegen. Abbildung 5 zeigt das Framework Coalition-X inklusive der wesentlichen Prozessschritte und Akteure. Je nach Prüfungsauftrag prüft der Wirtschaftsprüfer auf dieser Basis den Datenfluss sowie die grundlegende Methodik und Verarbeitung.

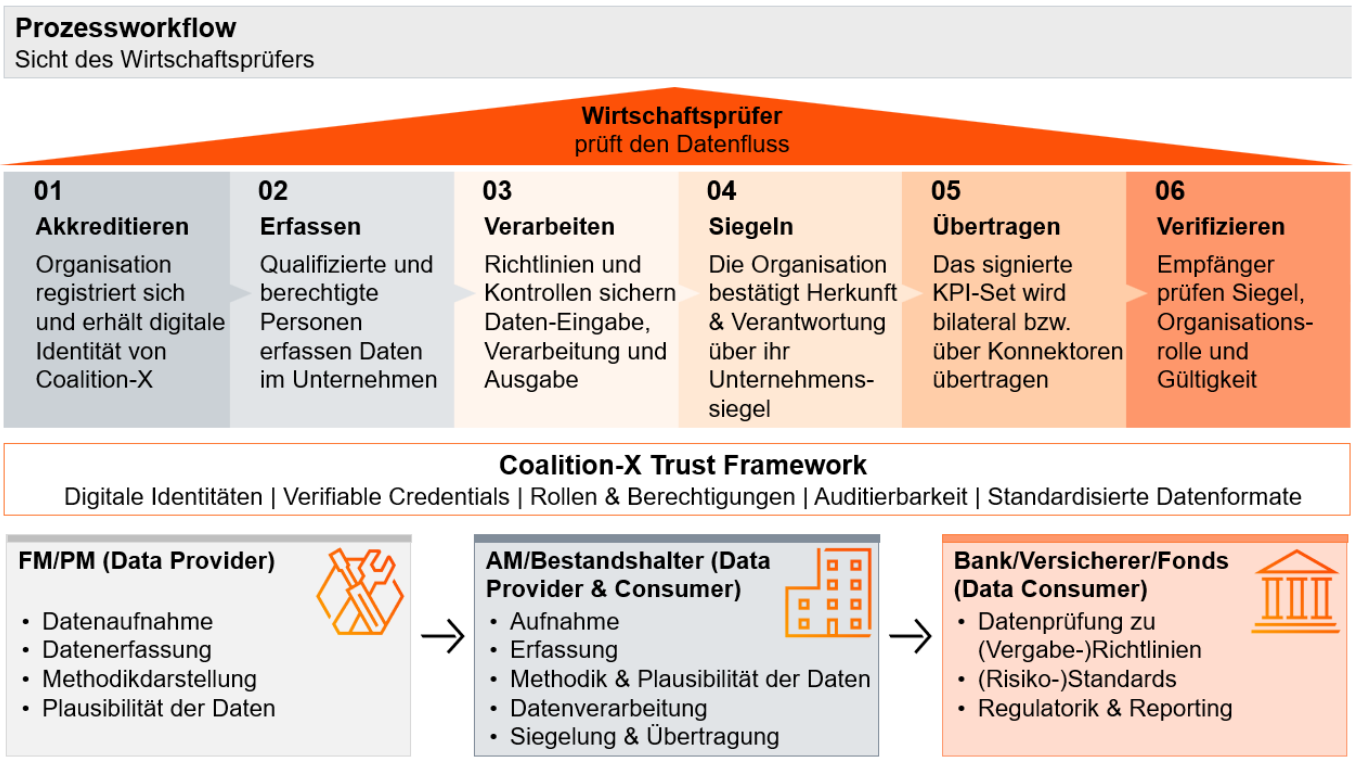


Abbildung 5: Prozessworkflow – kontrollierter Datenprozess von der Erfassung bis zur Weitergabe, Quelle: Coalition-X

Dazu sind im Wesentlichen folgende Fragen zu beantworten:

- **Wer verantwortet den Ursprungswert?**

Die Organisation, die den Wert originär erhebt oder aus einer Primärquelle übernimmt. Die Abgrenzung zwischen der Verantwortung für den Ursprungswert und der Verantwortung für die richtige und vollständige Übernahme ist in Abschnitt 2.1 („Verantwortung im Datenprozess“) beschrieben und sollte je Datenpunkt dokumentiert sein, wie es die dortige Übersicht vorsieht

- **Wer verantwortet die Verarbeitung?**

Jede Organisation für die Verarbeitungsschritte, die sie selbst vornimmt (Konsolidierung, Umrechnung, Zuordnung zu Berichtsperioden, Aggregation zu Kennzahlen). Werden gesiegelte Daten einer Vorstufe unverändert weitergereicht, bleibt die Verantwortung bei der Vorstufe; werden sie verändert oder zusammengeführt, entsteht eine eigene Verantwortung für den neuen Beitrag. Das Unternehmenssiegel macht diese Zäsur sichtbar; zur Verkettung der Siegel über mehrere Organisationen siehe das Praxisbeispiel in Kapitel 2.3 und den Abschnitt 3.3.3 „Credential und Unternehmenssiegel“.

- **Wer gibt Daten frei und wer darf siegeln?**

Freigabe und Siegelung sind organisatorisch zu trennen. Die fachliche Freigabe erfolgt nach den im IKS definierten, risikobasierten Kontrollregeln. Ein Vier-Augen-Prinzip ist insbesondere bei wesentlichen manuellen Änderungen, begründeten Auffälligkeiten oder festgelegten Freigaben aggregierter Daten vorzusehen, nicht jedoch pauschal für jeden Datenpunkt.

Die Siegelung ist dagegen eine Vertretungshandlung der Organisation: Mit dem Unternehmenssiegel ordnet der nach den Akkreditierungskriterien benannte Verantwortliche den Datensatz der Organisation zu, die damit die Verantwortung für Herkunft und Bereitstellung übernimmt. Als Governance-Regel empfiehlt sich, dass eine Siegelung nur nach dokumentierter, fachlicher Freigabe erfolgt sowie in einer internen Richtlinie oder Vollmachtsregelung festgelegt und im Berechtigungskonzept technisch abgebildet ist, wer siegeln darf. Eine Siegelung ohne vorherige Freigabe wäre ein Verstoß gegen das eigene IKS, der bei wiederholten Qualitätsverstößen bis zum Widerruf des Credentials führen kann.

3.1.2. Rollen und Verantwortungsgrenzen im Datenökosystem

Die Verantwortung von PM und FM ist auf den jeweils übernommenen Beitrag zur Datenkette begrenzt. Auftraggeber bzw. Asset Manager bleiben verantwortlich für die Festlegung des Datenbedarfs, der Berichtsgrenzen und der Methodik (etwa Flächendefinition, Bilanzgrenzen, Emissionsfaktoren), für die Bereitstellung der Primärquellen, auf die der Dienstleister angewiesen ist, sowie für die Berichterstattung selbst. Eine gesetzliche Berichtspflicht des berichtspflichtigen Unternehmens wird durch die Beauftragung eines PM- oder FM-Dienstleisters nicht auf diesen übertragen. Operative Aufgaben der Datenerhebung, -verarbeitung und -bereitstellung können dagegen vertraglich delegiert werden.

Der technische Plattformanbieter (Technical Service Provider) verantwortet Verfügbarkeit, Integrität und Sicherheit der Übertragung sowie die korrekte technische Umsetzung von Signatur und Verifikation. Er übernimmt keine fachliche Verantwortung für den Inhalt der Daten und darf diese nicht ohne Protokoll verändern. Diese Trennung sollte vertraglich ausdrücklich festgehalten werden, insbesondere wenn der Plattformanbieter zugleich mit einem Datenlieferanten oder Datenempfänger verbunden ist.

Der Datenempfänger, etwa Bank, Investor oder Reporting-Dienstleister, verantwortet die Verwendung der Daten in seinen eigenen Prozessen. Das Siegel entbindet ihn nicht von einer eigenen Plausibilisierung und von der Prüfung, ob die Daten für seinen Zweck geeignet sind. Er kann sich jedoch auf Herkunft und Integrität verlassen und Rückfragen aufgrund der automatisiert auslesbaren Metainformationen gezielter an die verantwortliche Organisation richten.

3.1.3. Umgang mit Datenkonflikten und Korrekturen

Weichen Daten verschiedener Quellen voneinander ab, ist zu klären, welcher Beitrag welcher Organisation betroffen ist. Für diesen Fall enthält Coalition-X eine Empfehlung; aus der Siegellogik folgt jedenfalls, dass eine Organisation einen abweichenden Wert nicht stillschweigend überschreibt, sondern als eigenen, von ihr verantworteten Beitrag kennzeichnet und Rückfragen an die ursprungsverantwortliche Organisation richtet Der gesiegelte Ursprungswert kann im Datenset als Historie weitergeführt werden.

Innerhalb der Organisation fehlt eine entsprechende Regel häufig. Ein wirksames IKS sollte daher eine Eskalationsregel enthalten: Erfasser melden Abweichungen, die Freigabestelle entscheidet auf Grundlage dokumentierter Kriterien (zum Beispiel Vorrang des geeichten Messwerts vor der Rechnung, Vorrang des Originaldokuments vor der Systemeingabe) und die Entscheidung wird mit Begründung protokolliert. So bleibt erkennbar, welcher Wert letztlich freigegeben wurde, auf welcher Grundlage die Entscheidung erfolgte und welche ursprünglichen Informationen zugrunde lagen.

3.2. Datenqualität als vertraglich definierte Leistung

Datenqualität lässt sich nur verantworten, wenn sie definiert ist. Leistungsbilder und Verträge zwischen Auftraggeber und PM / FM sollten daher festlegen, welche Datenpunkte in welcher Erfassungsart, Frequenz und Granularität zu liefern sind, welche Qualitätsmerkmale (Vollständigkeit, Richtigkeit, Aktualität, Nachvollziehbarkeit) gelten und welche Nachweise mitzuliefern sind. Ohne diese Festlegung bleibt unklar, ob eine Abweichung ein Leistungsmangel oder ein hinzunehmender Unsicherheitsbereich ist. Bestehende Verträge und Leistungsbilder sollten daraufhin überprüft und, soweit erforderlich, entsprechend konkretisiert werden.

3.3. Nachweisführung im Coalition-X-Ökosystem

Die im vorangehenden Kapitel beschriebenen Kontrollen bilden die operative Grundlage für verlässliche ESG-Gebäudedaten. Coalition-X knüpft hieran mit einem organisationsbezogenen Trust Framework an, in dem Anforderungen an teilnehmende Organisationen, Datenflüsse und digitale Nachweise miteinander verbunden werden.

3.3.1. Akkreditierung von Organisationen und Rollen

Akkreditiert wird die einzelne juristische Person. Beschäftigte und Beauftragte handeln unter ihrer Verantwortung und erhalten keine eigenen Coalition-X-Credentials. Für PM- und FM-Unternehmen ist insbesondere die Rolle des Data Providers relevant, der Daten bereitstellt und deren Qualität und Richtigkeit verantwortet. Wer Daten anderer Organisationen bezieht, kann zusätzlich als Data Consumer auftreten. Betreibt ein Unternehmen eine angebundene technische Plattform, kommt die Rolle des Technical Service Providers (TechSP) hinzu. Mehrfachrollen sind möglich; ihre jeweiligen Anforderungen gelten nebeneinander.

3.3.2. Datenmanagement und Kontrollprozesse

Neben dem Nachweis der rechtlichen Existenz, der Benennung eines operativen Kontakts und eines vertretungsbefugten, eIDAS-identifizierten Sealing-Managers stehen die Datenprozesse im Mittelpunkt. Für Data Provider bildet ein dokumentiertes internes Kontrollsystem den organisatorischen Rahmen. Aus

ihm muss hervorgehen, wer Daten erfasst, verarbeitet, prüft und freigibt und wie Fehler, Änderungen und Berechtigungen behandelt werden.

Der Kriterienkatalog betrachtet hierfür vier Prozessbereiche:

1. Datenaufnahme und Erfassung
2. Datenhaltung und Speicherung
3. Datenverarbeitung und Qualitätssicherung
4. Datenübergabe und Transfer

Für PM und FM bedeutet dies beispielsweise: Eingabeanforderungen und zulässige Quellen festlegen, nur autorisierte und unterwiesene Personen einsetzen, Eingaben plausibilisieren, Verarbeitungsschritte dokumentieren, Ergebnisse kontrollieren und Korrekturen nachvollziehbar protokollieren. Hinzu kommen geschützte Speicherung, geregelte Zugriffsrechte und die kontrollierte Weitergabe an autorisierte Empfänger. Die im vorangehenden Kapitel dargestellten Maßnahmen je Datenpunkt konkretisieren diese übergeordneten Unternehmensprozesse, etwa für Zählerstände oder die Übernahme von Energieausweisdaten. Die Akkreditierung selbst bezieht sich ausdrücklich auf die Organisation und ihre rollenbezogenen Prozesse, nicht auf die Einzelprüfung jedes Messwerts oder jeder Kennzahl.

3.3.3. Credential und Unternehmenssiegel

Bei der Akkreditierung beschreibt die Organisation anhand standardisierter Abfragen, wie sie die jeweilige Anforderung erfüllt, stellt stützende Dokumentation bereit und benennt einen Ansprechpartner. Ein hierfür anerkannter Standardnachweis (z. B. ISO/IEC 27001, BSI C5 oder SOC 2) kann die eigene Dokumentation ersetzen, sofern er das betreffende Kriterium und den erforderlichen Geltungsbereich abdeckt.

Nach erfolgreicher Zulassung erhält die Organisation ein maschinenlesbares Akkreditierungs-Credential (Verifiable Credential, VC). Es weist ihre Identität, Rollen, Berechtigungen und die Gültigkeit der Zulassung nach. Es ist die Grundlage für das elektronische Unternehmenssiegel, das über einen Vertrauensdienstanbieter bereitgestellt wird. Das Credential belegt die Zulassung; das Siegel macht Herkunft und Integrität der gesiegelten Daten überprüfbar.

Die Herkunftsnachweise können über mehrere Organisationen hinweg miteinander verknüpft werden. So kann ein Datensatz bereits die Unternehmenssiegel von Facility Manager, Property Manager, Asset Manager und weiteren beteiligten Datenlieferanten enthalten, bevor er den abschließenden Datenempfänger, etwa eine Bank, erreicht. Jede Organisation siegelt dabei die von ihr verantworteten Daten bzw. den von ihr zusammengestellten Datensatz. Bereits vorhandene Nachweise der Vorstufen bleiben erhalten und werden mit den nachfolgenden Beiträgen verknüpft. Werden Werte verändert oder zu neuen Kennzahlen aggregiert, werden Ursprung und Verarbeitung nachvollziehbar. Der Empfänger

kann dadurch die Herkunft und Integrität der jeweiligen Beiträge sowie die zugehörigen Akkreditierungsnachweise entlang der Datenkette prüfen.

Die drei Begriffe Credential, Zertifizierung und Assurance werden in der Praxis häufig vermischt, bezeichnen aber unterschiedliche Aussagen mit unterschiedlicher Reichweite. Das Coalition-X-Credential bestätigt die Zulassung einer Organisation für ihre Rolle, insbesondere das Vorhandensein dokumentierter Datenprozesse und eines IKS (zum Verfahren siehe Abschnitt 3.3 „Nachweisführung im Coalition-X-Ökosystem“). Es ist eine Aussage über die Organisation, nicht über einzelne Daten, und beruht auf Selbstauskunft und eingereichter Dokumentation.

Eine Zertifizierung, etwa nach ISO 9001 oder ISO/IEC 27001, bestätigt durch einen unabhängigen Dritten die Konformität eines Managementsystems mit einem definierten Standard. Welche Zertifikate im Akkreditierungsverfahren als Standardnachweis anerkannt werden, ergibt sich aus dem Kriterienkatalog (siehe „Credential und Unternehmenssiegel“). Auch sie beziehen sich auf Prozesse, nicht auf die Richtigkeit konkreter Werte.

Assurance bezeichnet die Prüfung eines Datensatzes oder Prozesses durch einen unabhängigen Prüfer, in der Regel einen Wirtschaftsprüfer, nach einem anerkannten Prüfungsstandard (etwa ISAE 3000 (Revised), ISAE 3410 für Treibhausgasangaben oder ISSA 5000 für Prüfungen von Nachhaltigkeitsinformationen, wirksam ab dem 15. Dezember 2026) mit einem Prüfungsurteil. Nur sie trifft eine Aussage zur inhaltlichen Richtigkeit innerhalb des gewählten Sicherheitsniveaus.

3.3.4. Laufende Gültigkeit und Compliance

Weder Credential noch Unternehmenssiegel garantieren die inhaltliche Richtigkeit jedes Datenpunkts. Die fachlichen Kontrollen im Unternehmen und eine gegebenenfalls erforderliche unabhängige Prüfung bleiben eigenständige Aufgaben.

Bei jeder Datentransaktion bzw. bei jedem Signier- oder Verifizierungsschritt prüft der Trust Layer automatisiert, ob das in den Daten enthaltene Akkreditierungs-Credential gültig ist, ob die erforderlichen Berechtigungen vorliegen und ob die Signatur einer vertrauenswürdigen Identität zugeordnet werden kann.

Compliance wird neben der jährlichen Akkreditierungsprüfung auch über laufende Status- und Gültigkeitsprüfungen abgesichert. Bei wiederholten Datenqualitätsverstößen, Sicherheitsvorfällen oder Verletzungen der Akkreditierungskriterien kann die Coalition-X den Status eines Credentials widerrufen. Ab diesem Zeitpunkt würden neu verifizierte Datensätze dieses Teilnehmers als ungültig oder nicht vertrauenswürdig gekennzeichnet; der Datenempfänger kann dann gezielt die Integrität beim ursprünglichen Data Provider nachprüfen. Da dieser seine Verarbeitungsaktivitäten protokollieren muss, können Probleme leicht identifiziert (und behoben) werden.

Für PM- und FM-Organisationen verbindet die Akkreditierung damit drei Ebenen: dokumentierte Verantwortlichkeiten und Kontrollprozesse im Unternehmen, rollenbezogene Nachweise für die Teilnahme sowie digital prüfbare Herkunfts- und Integritätsnachweise bei der Datenweitergabe. Der praktische Nutzen liegt darin, diese Grundlagen entlang der Datenkette nachvollziehbar und maschinenlesbar zu machen. Die Qualitätssicherung am Ursprung und die Verantwortung der beteiligten Organisationen bleiben dafür unverzichtbar.

3.4. Von Vertrauensnachweisen zur unabhängigen Prüfung

Der Wirtschaftsprüfer prüft in der Regel die Nachhaltigkeitsberichterstattung des berichtspflichtigen Unternehmens, nicht den Dienstleister; die Daten von PM und FM sind für ihn Prüfungsgegenstand entlang der Datenkette. Dass er sich nach einer Beurteilung von Angemessenheit und Wirksamkeit auf die Kontrollen des Dienstleisters stützen und eigene Prüfungshandlungen reduzieren kann, ist in den Abschnitten 2.3 und 2.6 dargestellt. Für die Governance folgt daraus: Ein dokumentiertes IKS mit Protokollen, Stichprobennachweisen und klaren Freigaben ist der wichtigste Beitrag des Dienstleisters zu einer effizienten Prüfung.

„Die Prüfungstiefe hängt vom vereinbarten Sicherheitsniveau ab; Abbildung 6 veranschaulicht die Unterschiede zwischen begrenzter und hinreichender Sicherheit. Bei begrenzter Sicherheit (limited assurance), die nach der Omnibus-I-Richtlinie (EU) 2026/470 das Prüfungsniveau für die CSRD-Berichterstattung bleibt (die Einführung von reasonable assurance wurde gestrichen; harmonisierte Standards für limited assurance sind bis Juli 2027 vorgesehen), stehen Befragungen, analytische Prüfungshandlungen und die Beurteilung des Prozessdesigns im Vordergrund. Bei hinreichender Sicherheit kommen Funktionsprüfungen der Kontrollen und umfangreichere Einzelfallprüfungen hinzu.

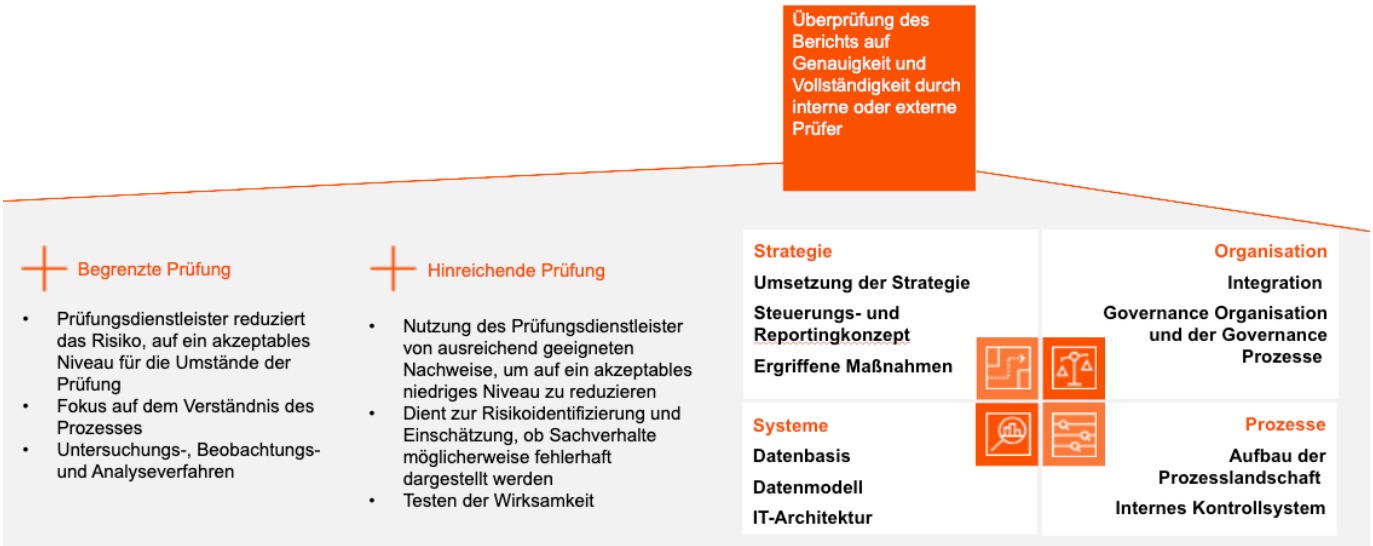


Abbildung 6: Begrenzte vs. hinreichende Prüfung, PwC

Wirtschaftsprüfer können Zertifikate und Prüfberichte Dritter verwerten, etwa ein Zertifikat über das Managementsystem oder einen Bericht über dienstleistungsbezogene Kontrollen nach ISAE 3402

beziehungsweise IDW PS 951; diese ersetzen jedoch nicht die eigene Urteilsbildung. Für Dienstleister mit großen Portfolien könnte ein solcher Kontrollbericht künftig ein Weg sein, Mehrfachprüfungen durch die Prüfer verschiedener Auftraggeber zu vermeiden; in der FM-Praxis ist dies soweit ersichtlich bislang nicht etabliert.

3.5. Haftung und Umgang mit nachträglich erkannten Fehlern

Mit der Verantwortung für einen Datenbeitrag geht ein Haftungsrisiko einher. Gegenüber dem Auftraggeber haftet der Dienstleister nach den vertraglichen Regelungen für Mängel seiner Leistung, mithin für fehlerhafte, unvollständige oder verspätete Daten, soweit er sie zu vertreten hat. Das Unternehmenssiegel begründet keine darüber hinausgehende Garantie für die inhaltliche Richtigkeit und keine unmittelbare vertragliche Beziehung zum abschließenden Datenempfänger. Ob eine Haftung gegenüber Dritten in Betracht kommt, hängt von den Umständen ab, etwa davon, ob der Dienstleister erkennbar auch zugunsten eines bestimmten Datenempfängers tätig wird.

Verträge sollten daher Leistungsumfang, Qualitätsmerkmale und Verantwortungsgrenzen klar beschreiben, Haftungsbegrenzungen vorsehen, soweit zulässig, und regeln, wie mit nachträglich erkannten Fehlern umzugehen ist (Korrektur, Information der Empfänger, erneute Siegelung). Zugleich ist ein dokumentiertes und gelebtes IKS der beste Schutz: Wer nachweisen kann, dass er die vereinbarten Kontrollen durchgeführt hat, kann sich gegen den Vorwurf einer Pflichtverletzung verteidigen. Governance ist damit nicht nur Voraussetzung für die Akkreditierung, sondern auch Risikovorsorge.

4. Vom Datenlieferanten zum Trusted Data Provider - Handlungsbedarf und Ausblick

4.1. Gemeinsamer Handlungsbedarf entlang der Wertschöpfungskette

Belastbare ESG-Daten entstehen im Gebäudebetrieb – ihre Bedeutung reicht jedoch weit darüber hinaus. Sie unterstützen die Steuerung von Immobilien, Investitionsentscheidungen, Finanzierung und Berichterstattung. Dieses Whitepaper zeigt: Entscheidend ist nicht allein der einzelne Datenwert, sondern eine nachvollziehbare Kette aus Erhebung, Verarbeitung, Kontrolle und Weitergabe. Property und Facility Management übernehmen dabei eine Schlüsselrolle. Die Entwicklung vom Data Provider zum Trusted Data Provider ist deshalb keine reine Technologiefrage, sondern eine Weiterentwicklung von Leistungen, Prozessen und Verantwortung.

Die Motivation hinter Coalition-X verdeutlicht den gemeinsamen Handlungsbedarf: Vor allem Banken benötigen nachvollziehbare Gebäudedaten für ihr Risikomanagement und die Erfüllung

aufsichtsrechtlicher Anforderungen. Eigentümer und Investoren brauchen belastbare Informationen, um Finanzierungen vorzubereiten, Risiken zu bewerten und ihre Bestände weiterzuentwickeln. Asset, Property und Facility Manager müssen hierfür Datenqualität und anschlussfähige Prozesse sicherstellen. Wirtschaftsprüfer wiederum benötigen nachvollziehbare Nachweise und Kontrollpfade. Diese Anforderungen bestehen nicht allein aufgrund einzelner Berichtspflichten; auch regulatorische Vereinfachungen beseitigen den Informationsbedarf für Finanzierung und Risikosteuerung nicht.

Datenmengen und Nachweisanforderungen lassen sich dabei immer weniger wirtschaftlich durch Tabellen, individuelle Abfragen und manuelle Prüfungen bewältigen. Die Ziele „Aufwand reduzieren und Risiken kontrollieren“ verbinden daher die Interessen der Beteiligten. Sie werden jedoch nur erreicht, wenn Qualitätssicherung nicht an das Ende der Datenkette verlagert wird, sondern dort erfolgt und dokumentiert wird, wo Daten entstehen oder verändert werden. Das Facility Management wird nicht nur als Datenlieferant, sondern zunehmend auch als Datenmanager, Qualitätssicherer und aktiver Nutzer von Gebäudedaten gefragt ist.

Handlungsfelder im Property und Facility Management

Leistungsbilder und Verträge weiterentwickeln: Strukturierte und auditierbare Datenbereitstellung ist eine definierbare Leistung. Umfang, Qualitätsanforderungen, Nachweise, Übergabestellen sowie Zugriffs- und Nutzungsrechte müssen vertraglich abgebildet werden. Auch Mitwirkungspflichten, Fehlerkorrekturen, Verantwortungsgrenzen und die Vergütung zusätzlicher Leistungen sind zu regeln. PM und FM verantworten ihren Beitrag zur Datenkette, übernehmen aber nicht pauschal die Berichts- oder Prüfpflichten nachgelagerter Akteure.-

Datenkompetenzen und organisatorische Fähigkeiten aufbauen: Steigende Anforderungen an Datenqualität, Dokumentation und Nachweisführung erfordern geeignete personelle und organisatorische Voraussetzungen. Mitarbeitende im PM und FM müssen Datenquellen, Erhebungsverfahren und Qualitätsanforderungen verstehen und digitale Systeme sicher anwenden können. Dafür braucht es klare Rollenprofile, gezielte Qualifizierung und ausreichende Ressourcen. Datenmanagement ist fest in die operative Leistungserbringung sowie in bestehende Organisations- und Verantwortungsstrukturen zu integrieren.

Datenanforderungen und Verantwortlichkeiten klären: Gemeinsam mit Auftraggebern sind benötigte Datenpunkte, Quellen, Bezugsgrößen, Erhebungsintervalle und Qualitätsmerkmale festzulegen. Dabei ist zwischen der Verantwortung für Ursprungswerte, der korrekten Übernahme fremder Daten und eigenen Verarbeitungsschritten zu unterscheiden. Datenlücken und Abhängigkeiten, etwa von Mietern, Versorgern oder Messdienstleistern, müssen transparent gemacht werden.

Systeme anschlussfähig und Prozesse resilient gestalten: Bestehende CAFM-, ERP- und ESG-Systeme sollten auf standardisierte Datenmodelle, maschinenlesbare Nachweise und sichere Schnittstellen vorbereitet werden. Gleichzeitig sind Informationssicherheit, Datensicherung, Wiederherstellbarkeit und Notfallmanagement in die Datenprozesse zu integrieren. Anforderungen aus NIS-2 und dem KRITIS-Regelungsrahmen sind zu berücksichtigen. Resilienz betrifft auch Personal, Ersatzverfahren und Abhängigkeiten von Dienstleistern.

Daten für die operative Steuerung und Optimierung nutzen: Strukturiert erfasste und bereitgestellte Daten sollten nicht nur externen Berichts- und Prüfanforderungen dienen. Verlässliche Gebäude- und Betriebsdaten sind zugleich Grundlage für eine effizientere Steuerung von Energieverbräuchen, technischen Anlagen, Instandhaltung und Dienstleisterleistungen. PM und FM sollten gemeinsam mit Auftraggebern geeignete Anwendungsfälle identifizieren und datenbasierte Auswertungen in bestehende Steuerungsprozesse integrieren, um aus besserer Datenqualität konkrete Mehrwerte zu erzielen.

Kontrollen und Nachweisführung im Tagesgeschäft verankern: Grundlage verlässlicher Datenprozesse ist ein dokumentiertes, risikobasiertes internes Kontrollsystem. Plausibilitäts- und Vollständigkeitsprüfungen, Freigaben und Korrekturen sollten möglichst systemgestützt erfolgen und nachvollziehbar protokolliert werden. Statt jeden Datenpunkt manuell zu prüfen, kommt es auf angemessene Kontrollen, klar geregelte Verfahren für Auffälligkeiten, qualifizierte Mitarbeitende und eindeutige Zuständigkeiten an.

Datenverfügbarkeit und Messinfrastruktur verbessern: Verlässliche Daten erfordern die ausreichende Erfassung und eindeutige Zuordnung relevanter Gebäude- und Betriebsdaten. Bestehende Mess-, Zähler- und Erfassungskonzepte sind gemeinsam mit Auftraggebern auf Vollständigkeit, Genauigkeit und digitale Anschlussfähigkeit zu prüfen, um fehlende Messpunkte, uneinheitliche Verfahren und unklare Zuordnungen zu Gebäuden, Flächen oder Nutzungen systematisch zu erkennen. Technischer Anpassungs- und Investitionsbedarf sowie Zuständigkeiten sind transparent darzustellen und abzustimmen.

Die Umsetzung schrittweise erproben: Ein geeigneter Einstieg ist ein abgegrenzter Anwendungsfall, beispielsweise der Energie-Datenfluss ausgewählter Gebäude. Gemeinsam mit Auftraggebern, Plattformanbietern und Datenempfängern lassen sich Datenmodelle, Kontrollen und Übergaben praktisch testen. Der Nutzen sollte anhand konkreter Ergebnisse bewertet werden: weniger Rückfragen, kürzere Bereitstellungszeiten, geringerer manueller Aufwand und besser nachvollziehbare Datenqualität.

4.2. Ausblick: Datenökosysteme gemeinsam gestalten

Datenökosysteme und Frameworks wie Coalition-X bieten die Perspektive, diese unternehmensbezogenen Maßnahmen in einer marktneutralen Brancheninfrastruktur zusammenzuführen. Gemeinsame Regeln, standardisierte Konnektoren und überprüfbare Herkunftsnachweise sollen bestehende Plattformen verbinden und qualitätsgesicherte Daten für mehrere berechtigte Empfänger nutzbar machen. Die weitere Entwicklung wird zeigen müssen, wie zuverlässig und wirtschaftlich dieser Ansatz im Zusammenspiel unterschiedlicher Systeme, Unternehmensgrößen und Datenanforderungen funktioniert.

Für das Property und Facility Management eröffnet sich die Möglichkeit, diese Entwicklung aktiv mitzugestalten. Praktische Erfahrungen aus dem Gebäudebetrieb sind unerlässlich, damit Standards und Akkreditierungsanforderungen umsetzbar bleiben. Perspektivisch können daraus zusätzliche Leistungen entstehen – etwa kontinuierliche Datenqualitätssicherung, standardisierte Nachweisbereitstellung oder datenbasierte Betriebsoptimierung. Akkreditierung und digitale Siegel unterstützen diese Entwicklung, ersetzen jedoch weder fachliche Kontrollen noch erforderliche unabhängige Prüfungen.

Der Aufbau belastbarer Datenprozesse sollte deshalb nicht auf die vollständige Etablierung eines Ökosystems warten. Wer Daten heute professionell steuert, absichert und dokumentiert, schafft Voraussetzungen für automatisiertes ESG-Reporting, kann vermeidbare Prüf- und Haftungsrisiken reduzieren und stärkt seine Position als verlässlicher Partner. So werden PM und FM zu zentralen Akteuren einer vernetzten, resilienten und datenbasierten Immobilienwirtschaft – vom Gebäude bis zur Bank.

Über die Autoren (alphabetisch)

Torsten Betz ist Vertriebsleiter bei **ROM Facility Solutions**. Seine Schwerpunkte liegen im Vertrieb von nachhaltigen Lösungen im Facility Management sowie in der Entwicklung und Umsetzung von Nachhaltigkeitsstrategien.

Annelie Casper ist Geschäftsführerin bei **gefma – German Facility Management Association**. Ihre Expertise liegt im Facility Management, Architektur und nachhaltiger Lebenszyklusbetrachtung bei Immobilien.

Robert Gussoni ist Senior Manager Green Real Estate Strategy & Products bei der **Apleona Group** und verantwortet das Green Real Estate Produktportfolio. Er bringt Erfahrung aus (nachhaltigen) Transformationsprogrammen in CRREM-Organisationen und im produzierenden Gewerbe mit.

Dr. Michael Hellwig ist Abteilungsleiter Innovation, Digitalisierung und Research beim **ZIA Zentraler Immobilien Ausschuss e.V..** Er ist Mitinitiator der ZIA-KPI-Liste und der Coalition-X.

Sebastian Kreutel ist Partner und Head of Real Assets Consulting bei **PwC Deutschland**. Seine Schwerpunkte liegen in der Beratung zu Strategie, Betrieb, Risiko, Regulierung und Nachhaltigkeit (u. a. CSRD, EU-Taxonomie und SFDR) für Real Assets und Fondsmanagement.

Prof. Dr.-Ing. Christian Meysenburg ist Professor für Immobilien- und Facility Management an der **SRH Hochschule Heidelberg** und Inhaber von **Meysenburg und Partner Ingenieure**. Seine Schwerpunkte liegen in Nachhaltigkeit, Facility Management sowie der strategischen Beratung im Immobiliensektor.

Frank Rüll ist Leiter Solutions und Startup bei **STRABAG PFS**. Seine Schwerpunkte liegen in innovativen Gebäudetechnologien, Energie- und Kreislaufwirtschaft sowie Facility Management.

Olga Scheiermann ist Managerin im Bereich Real Assets Consulting bei **PwC Deutschland.** Ihre Schwerpunkte liegen in Fonds-, Asset- und Property Management mit Fokus auf Regulatorik, Nachhaltigkeit und Financial Services.

Jörg Schielein, LL.M., ist Rechtsanwalt und **Partner** bei **RÖDL.** Seine Schwerpunkte liegen in der rechtlichen und organisatorischen Beratung rund um Facility Management in allen Sektoren sowie national wie international.

Marius Schröm ist Associate im Bereich Real Assets Consulting bei **PwC Deutschland**. Seine Schwerpunkte liegen in Nachhaltigkeitsstrategien für Corporate Real Estate- und Asset Managern.

Joanna Spassova ist Wirtschaftsprüferin und Director bei **PwC Deutschland**. Ihre Schwerpunkte liegen in Financial Services, Asset und Wealth Management sowie in der Prüfung nach HGB und IFRS.

Kai Ukena ist Senior Manager und Head of Real Estate Strategy & Operations Consulting bei **PwC Deutschland.** Seine Schwerpunkte liegen in der Beratung zu Strategie-, Organisations- und Geschäftsmodellentwicklung sowie Governance für Asset, Corporate Real Estate und Facility Management.

Abbildungs- und Tabellenverzeichnis

Abbildung 1: Elemente des ESG-Reporting-Prozesses, PwC 4
Abbildung 2: Coalition-X Trust Framework, Quelle: Coalition-X 7
Abbildung 3: Die Datenkette, Quelle: Coalition-X 7
Abbildung 4: Das Trust-Framework, Quelle: Coalition-X 8
Abbildung 5: Prozessworkflow – kontrollierter Datenprozess von der Erfassung bis zur Weitergabe, Quelle: Coalition-X 19
Abbildung 6: Begrenzte vs. hinreichende Prüfung, PwC 24

Tabelle 1: Praxisbeispiel - Energiedaten vom Zähler bis zum Drittsystem 12
Tabelle 2: Datenarten, typische Quellen und Methodendarstellung zur prüfsicheren Erhebung im Rahmen von Coalition-X / der ZIA-KPI-Liste 16