Fraunhofer CINES

Implikationen der europäischen Datenstrategie und -regulierung für die Energiewirtschaft

Whitepaper

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
API	Application Programming Interface
BDSG	Bundesdatenschutzgesetz
DA	Data Act
DAO	Datenaltruistische Organisation
DGA	Data Governance Act
DSGVO	Datenschutzgrundverordnung
DTH	Datentreuhänder
DVMD	Datenvermittlungsdienst

Management Summary

Mit dem Data Act (DA) und dem Data Governance Act (DGA) als Teil der Digitalen Strategie und der digitalen Dekade der EU-Kommission sind zwei wichtige Regulierungen beschlossen worden. Deren Implikationen auf die Energiewirtschaft werden in diesem Whitepaper diskutiert und an drei Anwendungsbeispielen veranschaulicht.

Die Energiewirtschaft steht durch die stark wachsende Zahl dezentraler Erzeugungs- und Verbrauchsanlagen und der Kopplung mit weiteren großen Sektoren Wärme und Mobilität vor besonderen Herausforderungen in der Digitalisierung und der Nutzung von Daten. Deshalb sind die Chancen und Risiken, die sich durch die zukünftige Datenregulierung ergeben von besonderem Interesse.

Die prägnanteste Änderung ergibt sich aus dem Data Act (DA) durch das Recht für Anlagenbetreiber, deren im Betrieb erzeugten Daten vom Hersteller zu erhalten und selbst oder über dritte Servicedienstleister zu Nutzen. Dies erweitert die Datenverfügbarkeit etwa für Betreiber von Windenergieanlagen und erlaubt die Verwendung mit Servicepartnern für die Optimierung von Betrieb und Instandhaltung. Dieser Verwertungsweg lässt sich auf den Betrieb anderer Anlagen übertragen.

Der Data Governance Act (DGA) setzt einen Rechtsrahmen für Datenspende- und Datentreuhandmodelle. Diese Modelle können energiewirtschaftlich interessant sein, um Nutzungsrechte von Messdaten von Verbrauchern zu erhalten, die z. B. anonymisiert und zweckbezogen verwendet werden können, um bessere und individuellere Lastprofile von Haushalten zu erzeugen.

Auch in der Elektromobilität kann ein Datentreuhandmodell ein Ansatz sein, um die starken Interessenkonflikte zwischen Automobilherstellern und energiewirtschaftlichen Anwendern bei der Nutzung von Batteriedaten von E-Fahrzeugen aufzulösen. Ein beidseitig akzeptierter Datenzugang schafft enorme Potentiale bei der Verfügbarkeit von Flexibilität aus der E-Fahrzeug-Flotte.

Den Chancen dieser und weiterer Anwendungen steht eine hohe Komplexität der Regulierung gegenüber. Insbesondere der DGA gibt Datentreuhändern umfangreiche Pflichten auf. Zusätzlich gestaltet sich die Entwicklung von Geschäftsmodellen für Datentreuhänder in der Praxis ohne öffentliche Anlaufförderung häufig schwierig.

Für Unternehmen ergibt sich aus der kommenden Regulierung insbesondere der Bedarf, eigene Digital- und Datenstrategien zu überprüfen oder neu zu entwickeln. Insbesondere im Anlagenbau entstehen darüber hinaus Aufwände für die Entwicklung und Bereitstellung zusätzlicher Schnittstellen für Kunden. Auf Branchenebene können Verbänden im Sinne von neutralen Datentreuhändern neue Rollen einnehmen. Dazu sollten Diskussionen in den Verbänden geführt, Ziele definiert und in geförderten Projekten umgesetzt werden. Gleichzeitig bedarf es einer Überarbeitung und Vereinfachung des DGA von politischer Seite, um mehr Freiräume bei der Umsetzung von Datentreuhand- und Datenvermittlungsdiensten zu schaffen.

1. Einleitung

Mit dem Data Act und dem Data Governance Act als Teil der Digitalen Strategie und der digitalen Dekade der EU-Kommission sind zwei wichtige Regulierungen beschlossen worden, um den Zugang und die Nutzung von Daten zu vereinfachen. Ziel der Regulierungen ist es, datengetriebene Innovationen zu unterstützen und bestehende Prozesse in verschiedenen Industriesektoren effizienter umzusetzen, um damit die Wettbewerbsfähigkeit zu stärken. Durch den Data Act sollen mehr Daten aus Produkten, die mit dem Internet vernetzt sind, verfügbar werden. Der Zugang soll transparent und fair auch für kleine und mittlere Unternehmen möglich sein. Der Data Act und der Data Governance Act stellen die Rahmenbedingungen für einen verbesserten Datenaustausch dar, liefern aber keine konkrete Umsetzung. Vor diesem Hintergrund soll das vorliegende White Paper die Rückwirkungen des Data Act und Data Governance Acts auf datengetriebene Innovationen in der Energiewirtschaft genauer beleuchten und mögliche Handlungsoptionen für Akteure in der Energiewirtschaft aufzeigen.

Die Energiewirtschaft steht aufgrund der stark wachsenden Zahl vernetzter Produkte wie dezentrale Erzeugungs- und Verbrauchsanlagen vor besonderen Herausforderungen in der Digitalisierung und der Nutzung von Daten. Auch die Kopplung von den Anwendungssektoren Wärme und Mobilität mit dem Stromsektor bedingt einen großen Datenbedarf zur Koordination. Die beiden Regulierungen haben daher eine besondere Relevanz für die Energiewirtschaft, da hier eine Vielzahl an vernetzen Geräten eingesetzt wird, die Daten generieren.

Die neuen Regulierungen bieten zahlreiche Chancen für Anlagenbetreiber von vernetzten Produkten, indem sie auf die im Betrieb erzeugten Daten ihrer Anlagen einen einfachen Zugriff vom Hersteller erhalten und diese Daten selbst oder über dritte Service-Dienstleister nutzen können. Die Nutzung von Daten kann z. B. zu optimierten Betriebsabläufen und damit zu Kosteneinsparungen führen. Darüber hinaus können durch den verbesserten Datenzugang neue Geschäftsmodelle entstehen, in dem auf Basis der Daten Produktverbesserungen angestrebt werden oder verbesserte Dienstleistungen beispielsweise zur Wartung von Anlagen entwickelt werden.

Gleichzeitig bringen die neuen Regulierungen auch zusätzliche Anforderungen und damit Risiken mit sich. Die erhöhte Verfügbarkeit und Nutzung von Daten erfordern robustere Datenschutz- und Sicherheitsmaßnahmen, um sensible Informationen vor Missbrauch zu schützen. Unternehmen müssen sicherstellen, dass sie in der Lage sind, die neuen gesetzlichen Anforderungen zu erfüllen und prüfen, welche Investitionen in IT-Infrastruktur und Fachwissen erforderlich sind. Für Hersteller von Anlagen, die mit dem Internet verbunden sind, ist es notwendig, zu prüfen, welche Daten ihre Anlagen erheben und in welcher Form sie diese auch zukünftig weiter nutzen können, wenn die Rechte ihrer Kunden als Anlagenbetreiber durch den Data Act gestärkt werden. Die Anforderungen für einen einfachen Zugang zu Anlagendaten kann neue Möglichkeiten für den Datenaustausch zwischen Unternehmen eröffnen und die Zusammenarbeit und Interoperabilität zwischen den Akteuren in der Energiewirtschaft stärken.

Vor diesem Hintergrund bieten der Data Act und der Data Governance Act bedeutende Möglichkeiten, die Digitalisierung und Datennutzung in der Energiewirtschaft voranzutreiben. Die Implikationen dieser Regulierungen sind vielschichtig und eröffnen energiewirtschaftlichen Akteure Chancen, die Wettbewerbsfähigkeit zu steigern aber bedingen auch Risiken, um die Anforderungen zu erfüllen. Dieses Whitepaper hat daher das Ziel, ein besseres Verständnis für die Auswirkungen der neuen Datenregulierung zu entwickeln und Wege aufzuzeigen, wie die Energiewirtschaft diese Veränderungen erfolgreich bewältigen kann.

2. Grundlagen zum Datenaustausch

2.1. Akteure beim Datenaustausch

Zentrale Akteure beim Datenaustausch sind die **Datennutzenden** und –die **Datengebenden**. Wie der Name sagt, stellen Datengebende ihre Daten den Datennutzenden zur Verfügung. Für die Nutzenden steht meist die Verfügbarkeit geeigneter Daten und die Qualitätsprüfung der Daten im Fokus, um die Daten in den eigenen Use Cases nutzen zu können. Für die Datengebenden ist regelmäßig eine einfache Weitergabe der Daten (Interoperabilität) und Vermeidung von Risiken (z. B. Abfluss von Geschäftsgeheimnissen) von höchster Bedeutung, sowie die Sicherung der Datenqualität.

Datentreuhänder sind Intermediäre, die diese beiden Parteien zusammenbringen und den Datenaustausch möglich machen und vereinfachen. Insbesondere sollen sie helfen, Vertrauen zwischen den Parteien herzustellen. Stand heute finden Experimente mit unterschiedlichen Datentreuhandmodellen in diversen Branchen statt, von Automotive und Mobilität bis Pflanzenzucht und Forstwirtschaft. Es hat sich jedoch noch kein allgemeingültiges Modell als optimal herauskristallisiert. Gleichwohl übernehmen oder unterstützen Datentreuhänder oft die Bereitstellung folgender Aufgaben und Funktionen:

- Sichere technische Infrastrukturen für den Datentausch
- Vertrauenswürdige Authentifizierung von Datennutzenden und Datengebenden
- Datenkataloge oder Portale, um Datenangebote zu finden
- Musterverträge und Standardklauseln für den Datenaustausch
- Zahlungsabwicklung und ähnliche Prozesse

Ambitioniertere Datentreuhänder können auch weitere Funktionen anbieten, z. B. aktives Matchmaking zwischen

Gebenden und Nutzenden, Entwicklung und Zertifizierung von Software-Tools und Lösungen und sogar die Orchestrierung umfassender Daten- und Entwicklerökosysteme.

Zwei wichtige Unterformen des Datentreuhänders sind der **Datenvermittlungsdienst** (DVMD) und die **Datenaltruistische Organisation** (DAO), die im Data Governance Act (DGA) definiert werden, und die gem. DGA teilweise umfangreichen Pflichten unterliegen (vgl. Kap. 2.5 unten). Nicht alle Datentreuhänder und Datenspendenorganisationen fallen allerdings zwangsläufig in den Geltungsbereich des DGA. Manche sind sogar explizit daraus ausgenommen, z. B. Datenbroker und Datentreuhänder die nur eine geschlossene (begrenzte) Gruppe von Gebenden und Nutzenden bedienen.

2.2. Datenkategorien und Datenquellen

Je nach ihrem Schutzbedarf können Daten zwei verschiedenen Kategorien zugeordnet werden: **offenen Daten** und **geschützten Daten**. Teilweise können diese wiederum in verschiedene Unterkategorien aufgeteilt werden. In welche Kategorie sie fallen, hat Implikationen für den Datenaustausch. Je weniger geschützt Daten sind, desto einfacher können sie geteilt werden. Eine weitere Kategorie, die zunehmend an Bedeutung gewinnt, sind **synthetische Daten**.

- **Offene Daten:** Daten, die ohne Einschränkung genutzt, weiterverbreitet und weiterverwendet werden dürfen.[1] Auch ursprünglich personenbeziehbare Daten, die anonymisiert worden sind – d.h., dass ihr Personenbezug **unumkehrbar** gebrochen wurde, so dass eine Reidentifizierung der Personen ausgeschlossen werden kann – gelten als nicht-personenbezogene Daten und können als offene Daten genutzt werden.
- **Geschützte Daten:** Alle weiteren Daten, die nicht öffentlich zugänglich und geschützt sind. Diese lassen sich nochmals nach dem Schutzgrund und der Schutzhöhe unterscheiden in:
- **Personenbeziehbare Daten:** Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, und somit in den Geltungsbereich der Datenschutzgesetze fallen (DSGVO, BDSG etc.).
  - **»Besondere Kategorien« personenbezogener Daten:** Art. 9 DSGVO führt eine Unterkategorie von besonders schutzwürdigen (da vermutlich besonders sensiblen) Daten ein, sog. »besondere Kategorien personenbezogener Daten«. Darunter fallen Daten aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische, biometrische und Gesundheitsdaten sowie Daten zu Sexualleben und sexueller Orientierung. Die Verarbeitung dieser Daten unterliegt besonders hohen Auflagen. Für die Energiewirtschaft dürften diese Daten jedoch selten relevant sein.
  - **Daten, die Geschäftsgeheimnisse enthalten:** Daten über bestimmte technische Systeme oder Prozesse enthalten oft kritische Geschäftsinformationen, z. B. Kennlinien von Batterien in der Energiespeicherindustrie. Firmen müssen jeweils für sich definieren, welche ihrer Daten unbegrenzte geteilt werden können, welche nur unter bestimmten Auflagen oder mit bestimmten Nutzenden, und welche so sensibel sind, dass sie keinen Externen verfügbar gemacht werden können.
  - **Synthetische Daten:** Daten, die künstlich generiert worden sind. Synthetische Daten werden auf Basis eines »echten« Datensets generiert. Das neue künstliche (synthetische) Datenset repliziert die Strukturen des ihm zugrundeliegenden ursprünglichen Sets, ohne dass aber einzelne »künstliche« Werte den ihnen zugrundeliegenden »echten« Werten zugeordnet oder Informationen, die diese identifizieren würden, aus dem künstlichen Datenset herausgelesen werden könnten. Synthetische Daten spielen in der KI-Entwicklung eine wachsende Rolle.

Es gibt eine Vielzahl von **Datenquellen**. Besonders wichtige für die Energiewirtschaft sind:

- Industrielle Produktions- und Anlagendaten
- Zeitreihen von Messdaten zum Strombezug von Haushalten und Unternehmen
- Öffentliche Daten von öffentlichen Stellen
- Forschungsdaten und Verbandsdaten

2.3. Datenlebenszyklus

Der Datenaustausch findet innerhalb des Datenlebenszyklus statt, der sich in 5 Schritten darstellen lässt (siehe Abbildung 1).

Der erste Schritt im Daten-Lebenszyklus ist die **(1) Datenerhebung.** Diese wird in der Regel vom Datengebenden übernommen und geschieht meist mittels Sensorik, gelegentlich (z. B. bei Haushalten) auch über manuelle Eingabe. Auch Softwareanwendungen können Daten erzeugen, die im Energiebereich relevant sind, z. B. Preisvorhersagen oder Transaktionsdaten von Energiemärkten.

Der nächste Schritt im Daten-Lebenszyklus ist die **(2) Aufbereitung oder Veredelung** der erhobenen Rohdaten, um sie für weitere Analysen und Verarbeitung verwendbar zu machen. Dieser Schritt umfasst insbesondere die **Bereinigung**

1 https://data.europa.eu/elearning/de/module1/#/id/co-01

Abbildung 1: Datenlebenszyklus aus Erhebung, Aufbereitung, Zugriff, Verarbeitung und Löschung

der Daten um Mess-, Einheiten-, Formats- und andere Fehler zu beseitigen; ihre **Formatierung** und ggf. **Annotierung** oder **Zusammenfassung** nach einem festgelegten Schema. Bei personenbezogenen Daten kann die Aufbereitung auch eine **Anonymisierung** oder **Pseudonymisierung** beinhalten, um die Einhaltung von Datenschutz und Datensicherheit zu gewährleisten. Gerade wenn die Daten geteilt werden sollen, ist dies wichtig. Aus dem gleichen Grund können bei nicht-personenbeziehbaren aber schutzbedürftigen Daten (z. B. Geschäftsgeheimnissen) kritische Informationen gelöscht werden.[2]

Sehr wichtig, wenn die Daten geteilt oder auch nur innerhalb der datenerhebenden Organisation breit verwendet werden sollen, ist die Erstellung **aussagekräftiger Metadaten**. Gute Metadaten ermöglichen Nutzenden, relevante Datensätze zu finden und schnell zu verstehen, welche Daten das Set beinhaltet, wie die Daten strukturiert, formatiert, annotiert und/oder gecodet sind; wie, von wem und wann sie erhoben wurden, ihre Qualität und Zuverlässigkeit, welche Einheiten verwendet werden, und wie die Rohdaten aufbereitet wurden.

Metadaten sollten nach definierten Standards und festen Vokabularien erstellt werden. Es existieren mittlerweile zahlreiche Metadaten-Standards.[3]

Werden die Daten geteilt, gewährt der Datengebende dem Datennutzenden nun **(3) Zugriff auf die Daten.** Konkret kann dies in der Maschine-zu-Maschine Kommunikation etwa über eine API geschehen oder in der Mensch-zu-Maschine Kommunikation über die Bereitstellung in einem Web-Portal oder über den Versand einer E-Mail. Der Nachteil dieses Weges für den Datengebenden ist, dass er alle praktische Kontrolle über die Daten aufgibt.

Alternativ können die Daten auch in einen gesicherten Datenraum hochgeladen werden, der unter der Kontrolle des Datengebenden oder eines Dritten (z. B. eines Datentreuhänders) steht. Die Verarbeitung der Daten durch den Nutzenden erfolgt dann in diesem Raum, so dass Gebende bzw. der vertrauenswürdige Dritte Aufsicht und Kontrolle über die Daten behalten. Schließlich kann der Datengebende dem Nutzenden gar keinen direkten Zugriff auf die Daten gewähren, sondern ihm nur erlauben, seine Algorithmen an den Datengebenden (oder den vertrauenswürdigen Dritten) zu schicken. Letztere implementieren diese Algorithmen dann an den Daten, und der Nutzende erhält nur das Ergebnis der Berechnungen zurück. In jedem Fall müssen der Datengebende, der Nutzende sowie etwaige Dritte (Treuhänder, weitere Dienstleister) organisatorische und technische Vereinbarungen treffen, damit die Daten sicher und in hoher Qualität bereitstehen und verarbeitet werden können.

Sobald die geteilten Daten für den Datennutzenden bereitgestellt worden sind, kann **(4) die Verarbeitung der Daten** erfolgen, um aus ihnen Wert zu generieren. Je nach Vereinbarung zwischen dem Datengebenden, Nutzenden und etwaigen Dritten, erfolgt schließlich die **(5) Löschung oder Archivierung der Daten.**

Bei jedem dieser Schritte stehen die Datengebenden und Datennutzenden vor verschiedenen Herausforderungen, um einen nahtlosen Datenaustausch im Energiesektor zu ermöglichen.

2.4. Herausforderungen beim Datenaustausch

2.4.1. Ökonomische Herausforderungen und Risiken

Verstärktes Teilen und gemeinsame Nutzung von Daten zwischen Unternehmen, staatlichen Stellen und sogar

2 Anonymisierung bzw. Löschung von Geschäftsdaten u. ä. geht per Definition mit einem Informationsverlust einher. Wie groß bzw. problematisch dieser Informationsverlust ist, hängt von der jeweiligen Fragestellung und den Details des Datensets ab. Es gibt statistische Techniken, um den zu erwartenden Informationsverlust zu berechnen.

3 Siehe z.B. https://rdamsc.bath.ac.uk/ https://www.dcc.ac.uk/guidance/standards/metadata/list

Haushalten sind wichtige Treiber für Wirtschaftswachstum, neue Geschäftsmöglichkeiten und das Erreichen von Transformationszielen wie der Energiewende. Die Daten- und Digitalisierungsstrategie der EU sowie mehrere neue EU-Verordnungen schaffen hierfür einen rechtlichen und politischen Rahmen.

Trotz seiner Potentiale ist Datenteilen jedoch kein Selbstläufer. Der Grund hierfür ist, dass Datengebende und Nutzende sich oft einem grundsätzlichen **Nutzen-Kosten-Risiken/ Unsicherheiten-Trilemma** gegenübersehen. Für Gebende wie Nutzende lohnt sich das Datenteilen, wenn der so für sie entstandene Wert (Nutzen) die Kosten und Risiken übersteigt. Es kann jedoch schwierig sein, ex ante abzuschätzen, ob dies der Fall ist. Um stärkeres Datenteilen zu forcieren, gilt es also, Kosten und Risiken zu senken, Nutzen zu erhöhen und Unsicherheiten zu reduzieren.

Für die Datennutzenden liegt der **Wert** (Nutzen) meist in zusätzlichen Umsätzen, Kostensenkungen oder Innovationen, die die geteilten Daten ermöglichen. Mögliche Nutzen für die Datengebenden sind z. B. Gebühren oder andere monetäre Entschädigungen, die sie für die Daten erheben können, reziprok gewährte Datenzugänge oder Produkte oder Dienste, die die Nutzenden mit den Daten entwickeln und ihnen verbilligt gewähren. Gebende können Datenzugang als gesellschaftlichen Beitrag auch ohne direkten wirtschaftlichen Vorteil gewähren, etwa als Datenspende oder aus PR-Gründen.

Wichtigste **Kosten** für beide Akteure ist meist der Personalaufwand, um die Daten zu teilen, aufzubereiten, auf Qualität zu prüfen und auszuwerten. Weitere Kosten entstehen durch den Aufwand, wertige Use Cases für die Daten zu identifizieren und umzusetzen, Vereinbarungen mit dem Datengeber bzw. Nutzer zu schließen, die Compliance zu sichern, sowie etwaige Investitionen in IT-Infrastruktur und mögliche Gebühren für den Datenzugang.

Die wichtigsten **Risiken** entstehen durch fehlenden Datenschutz und mangelnde Datensicherheit sowie fehlende Rechtssicherheit. Für Datengebende besteht das Risiko, dass ihre Daten zu illegitimen Zwecken oder von unbefugten Stellen ausgewertet werden oder Geschäftsgeheimnisse abfließen. Datennutzende laufen Gefahr, dass Fehler in den Daten oder Metadaten unerkannt bleiben und zu kostspieligen Folgefehlern führen, oder dass der von der Datennutzung erhoffte Mehrwert nicht realisiert wird. Ein typisches Beispiel ist, dass sich verändernde Datenqualität die Genauigkeit und Zuverlässigkeit von KI-Anwendungen erheblich beeinträchtigen kann. Schließlich haben beide Akteure das Risiko, dass Compliance-Verstöße des jeweils anderen auf sie zurückfallen und ihnen Rechts- oder Reputationsschäden verursachen.

Ein weiterer **Unsicherheitsfaktor** betrifft die Frage, welche werthaltigen Use Cases es gibt, welche Daten für diese benötigt werden, wie groß der abzuschöpfende Mehrwert und der dafür nötige Aufwand tatsächlich sind. Dies könnte insbesondere dort der Fall sein, wo branchen- oder domänenübergreifende Use Cases entwickelt werden sollen. Hier ist einerseits das Innovationspotential am größten, andererseits sind diese oft noch am wenigsten definiert. Die Identifikation und Entwicklung von Use Cases erfordert daher oft intensive Kommunikation und Zusammenarbeit zwischen potenziellen Partnern. Vertrauenswürdige Dritte können hier als Matchmaker eine wichtige Rolle spielen, um Datengebende und Nutzende zusammenzubringen und ihnen zu helfen, Use Cases zu identifizieren.

Intermediäre wie **Datentreuhänder** helfen, die Risiken und Kosten für Datengebende und Nutzende zu senken. Sie senken Suchkosten durch Matchmaking und die Bereitstellung gepflegter Datenkataloge und Portale, helfen die Vertrauenswürdigkeit der Parteien und die Sicherheit der Transaktionen zu garantieren, und unterstützen ihre technische, rechtliche und geschäftliche Abwicklung.

2.4.2. Datenstandardisierung

Die bereitgestellten Daten müssen vom Datennutzer interpretiert und weiterverarbeitet werden können. Deshalb ist die Nutzung von Standards von hoher Bedeutung. Nach Standards erhobene und bereitgestellte Daten erreichen einen größeren Markt, haben mehr Anwendungsmöglichkeiten und sind deshalb von höherem Wert.

Für den Energiesektor ergeben sich hier besondere Chancen, weil bereits umfangreich Prozesse und Datenformate im regulierten Bereich der Energiewirtschaft vereinbart sind und in den Unternehmen vorliegen. Im nicht-regulierten Bereich bestehen hier noch erhebliche Potentiale, zum Beispiel bei der Bereitstellung von Betriebsdaten von Anlagen oder auch bei der Kommunikation von Daten für aufkommende Prozesse wie der Flexibilitätsbereitstellung.

2.4.3. Herausforderungen beim Datenaustausch

Vor jeder Verarbeitung von Daten (Erhebung, Bereinigung, Analyse, Löschung etc.) und einem Datenaustausch muss sichergestellt sein, dass sie rechtlich zulässig ist. Das gilt insbesondere bei personenbeziehbaren Daten (vgl. Art. 6 i. V. m. Art. 5 DSGVO) aber auch bei nicht-personenbeziehbaren Daten, wenn sich dies aus z. B. urheber-, wettbewerbs- oder vertragsrechtlichen Vorschriften ergibt. Grundsätzliche Fragen, die meist vertraglich oder im Rahmen einer Datenschutzerklärung geregelt werden, sind z. B. die Zwecke, zu denen die Daten verarbeitet werden, inwiefern die Daten oder die Verarbeitungsergebnisse mit Dritten geteilt werden dürfen, Löschfristen und Sicherheitsmaßnahmen, sowie ggf. die Kompensation von Datengebenden.

Eine Herausforderung ist, dass aus Compliance-Versäumnissen des einen Partners rechtliche Risiken für den anderen entstehen können. Ist z. B. ein Verarbeitungszweck des Datennutzenden, oder sogar die Datenweitergabe selbst, nicht von der Datenschutzerklärung oder anderen vertraglichen Dokumenten des Datengebenden gedeckt, kann sich hieraus ein Compliance-Verstoß sowohl des Nutzenden wie des Gebenden ergeben. Grundsätzlich kann dieser Herausforderung über eine belastbare Vertragsgestaltung und vorherige rechtliche Prüfung der geplanten Datenzugriffe und Verarbeitungen begegnet werden. Auch vertrauenswürdige Dritte wie Datentreuhänder können einen geeigneten Rahmen für die Datengebenden und Datennutzenden geben, um dieser Herausforderung zu begegnen.

Datensicherheit:
Bei **industriellen Produktions- und Anlagedaten** ist die Gewährleistung der Datensicherheit von herausragender Bedeutung. In einer Befragung von Bitkom äußerten 47 Prozent der Unternehmen, die keine Daten teilen, Angst vor möglichem Missbrauch ihrer Daten (Bitkom 2023b). Deswegen spielen die Authentifizierung und Autorisierung eine entscheidende Rolle, um die Datenzugriffe zu kontrollieren und Datenmissbrauch und die Weitergabe von Geschäftsgeheimnissen zu verhindern.

Schutzmaßnahmen werden daher von Unternehmen und anderen Institutionen bereits als Teil ihrer allgemeinen Datensicherheitsstrategie implementiert und können für den Datenaustausch genutzt werden. Je nach Modalität des Datenteilens können Schutzmaßnahmen durch Datentreuhänder oder andere vertrauenswürdige Dritte übernommen werden.

Interoperabilität:
Für einen einfachen Datenaustausch stellt die Interoperabilität eine wichtige Anforderung und häufig eine Herausforderung dar. In der oben genannten Bitkom-Befragung gaben 26 Prozent der Unternehmen den Datenaustausch auf, da Daten nicht direkt kompatibel waren (Bitkom 2023b). Die Heterogenität der Datenformate ist auch innerhalb derselben Branchen weit verbreitet und soll durch den Data Act deutlich vereinfacht werden. Die Daten müssen in »umfassenden, strukturierten, allgemein verwendeten und maschinenlesbaren Formaten« (EU Com 2024)[4] zur Verfügung stehen. Daher stehen viele Unternehmen vor der Herausforderung, diese Anforderungen zu erfüllen. Dies umfasst die Datenaufbereitung nach geeigneten (Branchen-)Standards und auch mögliche Aktualisierungen, wenn Standards angepasst werden.

Schutzbedürftige Daten:
Für geschützte Daten (z. B. industrielle Produktions- und Anlagendaten oder personenbeziehbare Daten) ist die Umsetzung von Schutzmaßnahmen eine Herausforderung. Unternehmen müssen sicherstellen, dass keine Informationen weitergegeben werden, die die Rechte von Anlagenherstellern oder Nutzern verletzen und damit zu finanziellen Verlusten oder Entschädigungen führen können. Datenanbieter müssen daher technische Maßnahmen ergreifen, um sensible Informationen zu schützen und gleichzeitig die Nutzbarkeit der Daten zu gewährleisten. Sollen aggregierte Daten geteilt werden, ist sicher zu stellen, dass keine personenbeziehbaren Informationen daraus abgeleitet werden können. Bei Smart Meter Daten ist der Schutz personenbeziehbarer Daten z. B. durch eine geografische oder zeitliche Aggregation von Daten (Wagh, Mishra 2023) möglich. Für die Umsetzung des Schutzes sensibler Daten stehen technische Lösungen zur Verfügung, die Anforderungen der Datengebenden und -Nutzenden erfüllen können.

Widerrufsrecht von Datenspenden:
Bei personenbezogenen Daten spielen Datenspenden eine wichtige Rolle, weil es die Kosten für Datennutzenden sparen kann. Da solche Daten jedoch oft sensible Informationen über Einzelpersonen enthalten, müssen die Datennutzenden sicherstellen, dass die betreffenden Daten ordnungsgemäß gelöscht werden, wenn ein Datenspender einen Widerruf der gespendeten Daten verlangt oder die Spendenvereinbarung ausläuft. Werden die Daten anonymisiert, sind sie nicht länger personenbezogene Daten und somit nicht länger im Geltungsbereich der DSGVO, so dass Widerrufsrechte (sowie alle anderen DSGVO Regeln) entfallen.

Trilemma – Herausforderungen
Die größte Herausforderung für den Datenaustausch stellt das **Nutzen-Kosten-Risiken/Unsicherheiten-Trilemma** dar. Hierzu sind sowohl für Datengebende wie auch Datennutzende folgende Fragen zu beantworten:

1. Wie groß ist der Nutzen der Daten / welchen Wert haben sie?
2. Wie groß ist der nötige Aufwand, um die Daten teilen zu können (einschl. der nötigen Aufbereitung der Daten)?
3. Wie groß ist das potenzielle Risiko für den Datenaustausch, welche Unsicherheiten bestehen?

Während die Datengebenden vor allem das Nutzen-Kosten-Dilemma bewältigen müssen, haben Datennutzenden zusätzlich auch Herausforderungen die Datenqualität, Interoperabilität und das Widerrufsrecht zu gewährleisten.

Als Infrastruktur, welche einige der genannten Herausforderungen beim Datenaustausch lösen kann, sind Modelle und Konzepte für Datenräume als Plattform entwickelt worden,

4 Absatz 1 in Artikel 5, Data Act online unter http://data.europa.eu/eli/reg/2023/2854/oj (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828)

die bereits in verschiedenen Sektoren auch operativ genutzt werden. Datenräume repräsentieren dezentrale Datenökosysteme, die auf einen gemeinsamen Nutzen abzielen und auf gemeinsam vereinbarten Technologien und Normen beruhen, um die Interoperabilität der Daten und die Sicherheit des Datenaustauschs zu gewährleisten.

Um Herausforderungen des Teilens und des Austausches von Daten zu lösen, sind Datentreuhänder eine Lösungsmöglichkeit, die als neutrale Dienstleister zwischen Datengebenden und Datennutzern agieren. Neben dem sicheren Datenaustausch auch über eigene Datenräume können Datentreuhänder weitere Herausforderungen lösen (u. a. Einhaltung von Compliance-Anforderungen, Aufbereitung von Daten z. B. zur Anonymisierung, Broker/Matchmaker zwischen Datengebenden und Nutzenden oder Beratungsdienstleistungen).

2.5. Lösungen zum Datenteilen durch EU-Regulierung

2.5.1 Data Governance Act (DGA)

Was sind die Ziele des DGA und wie sollen sie erreicht werden?
Der DGA trat im Juni 2022 in Kraft und wird seit 24. September 2023 angewendet. Er hat zwei wesentliche Ziele. Erstens will er das Teilen und Spenden von Daten unter Privaten sowie die Nutzung geteilter oder gespendeter Daten befördern. Der DGA führt die bisher geringe Bereitschaft von Firmen, Privatpersonen und sonstigen Akteuren der Datenwirtschaft, ihre Daten zu teilen, zu spenden oder solche Daten zu nutzen, auf mangelndes Vertrauen zurück. Daher entwickelt der DGA einen Rechtsrahmen für sog. Datenvermittlungsdienste (DVMDs; *data intermediary organisations*), die kommerzielles Datenteilen ermöglichen sollen, und für sog. Datenaltruistische Organisationen (DAOs; *data altruism organisations*), die Datenspenden forcieren sollen. DVMDs und DAOs können als Unterformen von Datentreuhändern verstanden werden. Der im DGA definierte Rechtsrahmen soll die Entstehung von vertrauenswürdigen DVMDs und DAOs befördern und so Abhilfe schaffen (European Commission 2024, Kerber 2021).

Zweites Ziel des DGA ist es, öffentliche Stellen, die im Besitz geschützter Daten sind, zu befähigen, diese zur Weiterverwendung herauszugeben. Öffentliche Stellen waren bereits durch die Open Data Directive (EU 2019/1024) angehalten, in ihrem Besitz befindliche Daten für die Nutzung durch Private freizugeben. Geschütze Daten – d.h. personenbeziehbare Daten, Geschäftsgeheimnisse, geistiges Eigentum und Daten unter Geheimhaltungspflicht – waren jedoch ausgenommen. Der DGA legt Bedingungen fest, unter denen solche Daten herausgegeben werden können. Er definiert aber keine neuen Rechtspflichten, diese Daten tatsächlich auch herauszugeben. Das bleibt den Mitgliedsstaaten vorbehalten. Wichtig ferner: Daten im Besitz von öffentlichen Unternehmen sowie Kultur- und Bildungseinrichtungen (z. B. Universitäten) sind von diesen Regelungen des DGA explizit ausgenommen. Für die Energiewirtschaft dürften daher vor allem die Regelungen zu DVMDs und DAOs relevant sein, weniger die zur Herausgabe öffentlicher Daten. Die weitere Diskussion fokussiert sich daher auf DVMDs und DAOs.

Was sind, was dürfen und was müssen Datenvermittlungsdienste?
Gem. Art. 2 DGA sind DVMDs Dienste, die *Geschäftsbeziehungen* zwischen einer *unbestimmten Anzahl* von Dateninhabern (Firmen, natürliche Personen, etc.) und Datennutzern herstellen, um *Datennutzung* zu ermöglichen. Explizit *keine* DVMDs sind:

i. Dienste wie Datenbroker, die Daten von Dateninhabern sammeln, diese wertsteigernd veredeln (z. B. anreichern, aggregieren) und an Datennutzer lizensieren, *ohne eine Geschäftsbeziehung zwischen Dateninhabern und Nutzern herzustellen*;
ii. Dienste, die ausschließlich von einem Dateninhaber (z. B. einem Großkonzern) genutzt werden, um die Verwendung seiner Daten zu ermöglichen (z. B. eine konzerninterne Datenplattform),
iii. Dienste, die von mehreren *juristischen* Personen in einer *geschlossenen Gruppe* genutzt werden (z. B. innerhalb einer Lieferkette);
iv. Anbieter technischer Werkzeuge wie Clouds oder Software, die Datenaustausche ermöglichen, deren Anbieter aber nicht als Vermittler auftritt. Ein Cloud-Anbieter ist also kein DVMD, ein Datenmarktplatz-Betreiber schon.

DVMDs können profit- wie nicht-profitorientiert sein. Art. 11 und 12 DGA regeln die Bedingungen für DVMDs. Diese sind relativ umfangreich. Die Wichtigsten sind:

- DVMDs müssen alle bestehenden gesetzlichen Bestimmungen einhalten, z. B. Datenschutz, Wettbewerbsrecht, Schutz von Geschäftsgeheimnissen, usw. Insbesondere hat der DGA keinen Vorrang vor der DSGVO.
- DVMDs dürfen die Daten, die Datengebende über sie teilen, zu keinen anderen Zwecken verwenden als (i) diese den Datennutzenden zur Verfügung zu stellen, (ii) um den Vermittlungsdienst selbst weiterzuentwickeln, und (iii) zu Sicherheitszwecken. Der DVMD darf die Daten also nicht für eigene geschäftliche oder sonstige Zwecke, die über die Datenvermittlung hinausgehen, nutzen.
- Der Gesetzgeber scheint vorzusehen, dass DVMDs die über sie ausgetauschten Daten grundsätzlich in dem Format weitergeben, in welchem sie sie von den Datengebenden erhalten haben. Formatumwandlungen sind grundsätzlich nur zulässig, um die Interoperabilität zu verbessern, auf Wunsch

der Nutzenden, aus rechtlichen Gründen oder um internationalen Datennormen zu genügen. Sonstige Datenveredelungen scheinen nur zulässig, wenn sie dem Datenaustausch dienen – genannt werden »Pflege«, Konvertierung, Anonymisierung und Pseudonymisierung – und bedürfen der ausdrücklichen Zustimmung der Datengebenden. Eine weitergehende Anreicherung der Daten mit zusätzlichen Informationen oder Aggregation zu einem größeren Datenprodukt könnte somit nicht zulässig sein und sollte zunächst rechtlich geprüft werden.

- Gleiches gilt für Zusatzdienste und Tools. Der DGA erwähnt, dass der DVMD solche anbieten könnte, scheint aber primär an Dienste/Tools zu denken, die direkt das Datenteilen erleichtern (z. B. Zwischenspeicherung, Anonymisierung). Ob weitergehende Dienste, z. B. Analytics, zulässig wären, ist noch unklar. Alle Anwendungen von Diensten/Tools bedürfen der Zustimmung der Datengebenden.
- DVMDs müssen gesonderte juristische Personen sein. Ein DVMD kann z. B. keine Geschäftseinheit innerhalb einer Firma sein, sondern müsste als eigenständige Tochtergesellschaft o.ä. organisiert werden. DVMDs dürfen Datengebenden und Nutzenden keine Sonderkonditionen (z. B. Rabatte) gewähren, wenn diese noch andere Dienste des DVMD oder von verbundenen Unternehmen nutzen.
- DVMDS müssen sich bei einer zuständigen Behörde anmelden, die jeder EU-Mitgliedsstaat benennt. In Deutschland übernimmt diese Funktion die Bundesnetzagentur. Diese Behörde gibt die Meldung unverzüglich an die Europäische Kommission weiter, die eine öffentliche Liste[5] anerkannter DVMDS führt.
- Weitere Vorschriften betreffen den fairen, transparenten und nicht-diskriminierenden Zugang, Sicherheit, Datenpannen, Informationspflichten, Insolvenz, Interoperabilität, Protokollierung und Datenübertragung ins Ausland.

DVMDS, die schon am 23. Juni 2022 ihre Dienste anboten, müssen den DGA ab 24. September 2025 erfüllen. DVMDS, die nach dem 23. Juni 2022 die Arbeit aufnahmen, wären grundsätzlich schon heute verpflichtet, den DGA zu erfüllen. In der Praxis ist das aktuell aber schon deshalb nicht vollständig möglich, da Deutschland die zuständige Behörde erst kürzlich benannt hat. EU-weit sind auch erst wenige DVMDS (u. a. aus Finnland, Frankreich und Ungarn) der Kommission gemeldet worden. Anerkannte DVMDs dürfen ein gemeinsames Logo[6] als »EU Recognised Data Intermediary« tragen.

Was sind, was dürfen und was müssen Datenaltruistische Organisationen?

Datenaltruistische Organisationen (DAOs) sind juristische Personen, die auf Grundlage von Datenaltruismus (»Datenspende«) bereitgestellte Daten erheben und Nutzenden für Ziele von allgemeinem Interesse zur Verfügung stellen (Art. 15 DGA). Art. 2, Abs. 16 DGA definiert »Datenaltruismus« als freiwillige, über Kostenentschädigung hinaus unentgeltliche Bereitstellung von Daten durch Dateninhaber bzw. natürliche Personen auf Grundlage einer Einwilligung, für Ziele von allgemeinem Interesse, wie der Bekämpfung des Klimawandels, Verbesserung der Mobilität, oder zur Forschung. Dabei lässt der DGA offen, ob gewinnorientierte Unternehmen solche gespendeten Daten verwenden dürfen, und wenn ja, ob für Zwecke mit zumindest mittelbarer Gewinnabsicht (z. B. Produkt-F&E). Der DGA schließt das zumindest nicht aus. In jedem Fall dürfen Datenspender nicht für ihren Altruismus entlohnt werden (egal, ob über Entgelte, Rabatte, Zugänge zu besonderen Dienstleistungen etc.).

Art. 19 DGA ermöglicht DAOs, sich als *»in der Union anerkannte«* DAO bei einer mitgliedsstaatlichen Behörde registrieren zu lassen (in Deutschland wieder die Bundesnetzagentur*). Anerkannte* DAOs dürfen sich als »EU Recognised Data Altruism Organisation« bezeichnen, ein entsprechendes Logo tragen, und werden in einem gemeinsamen europäischen Register geführt. Die Eintragung als »anerkannte DAO« ist aber *explizit kein Muss* – auch »nicht-anerkannte« Organisationen können weiterhin datenaltruistische Tätigkeiten durchführen (ErwG 46 DGA).

Die Bedingungen für eine Anerkennung sind relativ umfangreich (Art. 18–21 DGA). Anerkannte DAOs dürfen keine Erwerbszwecke verfolgen und müssen von jeder Organisation mit Erwerbsabsicht unabhängig sein. Ihre Dokumentations- und Berichtspflichten umfassen u. a. die Namen und Kontaktdaten aller Datengebenden und Datennutzenden, Zeitpunkt oder Dauer, Zwecke und technische Mittel der von den Nutzenden vorgenommenen Verarbeitungen und eingesetzten technischen Datenschutzmaßnahmen, sowie ggf. Ergebnisse. Die DAO muss die Datengebenden vor jeder Verarbeitung ihrer Daten über Ziele, Zweck und ggf. den Standort dieser informieren, und ihnen Werkzeuge zum einfachen Erteilen und Widerrufen von Einwilligungen bereitstellen. Hinzu kommen Sicherheitsanforderungen und Einhaltung eines noch durch die Kommission zu definierenden »Regelwerks«, das informations- und sicherheitstechnische Anforderungen weiter definieren soll (Art. 22 DGA). Ein Entwurf soll Anfang 2025 vorliegen. Die EU will auch ein gemeinsames Einwilligungsformular (*common consent form*) für DAOs herausgeben, so dass Einwilligungen unionsweit in standardisierter Form eingeholt werden können. Allerdings ist bislang erst eine einzige DAO (aus Spanien) im europäischen Register anerkannter DAOs erschienen.

5 Liste einsehbar unter https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services

6 Logo verfügbar unter https://digital-strategy.ec.europa.eu/de/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union

Was sind kritische Diskussionspunkte?
Das Ziel des DGA, stärkeres Teilen, Spenden und Nutzen von Daten zu forcieren, findet breite Unterstützung. Auch die Entwicklung eines EU-weiten Rechtsrahmens und gemeinsame europäische Logos und Brandings für DVMDs und DAOs ist grundsätzlich sinnvoll. Gleichzeitig wird kritisiert (z. B. Veil 2021a, 2021b, 2021c), dass der DGA in erster Linie neue und aufwendige Pflichten für DVMDs wie DAOs schafft, ohne im Gegenzug wesentliche Erleichterungen (z. B. Ausnahmen aus der DSGVO) oder Vorteile zu bieten. Diskutabel scheint auch die den DGA begründende Problemwahrnehmung, dass primär *mangelndes Vertrauen in ihre Sicherheit und Neutralität* die Entwicklung von DVMDs und DAOs hemme. Wie aber oben erläutert, schaffen Vertrauen/Neutralität noch keinen positiven Anreiz, Daten zu teilen. Erst die Erwartung, dass der Nutzen die Kosten überwiegen wird, schafft solche Anreize. Der (kostentreibende) Aufwand, den der DGA den DVMDs und DAOs auferlegt, sowie seine Einschränkungen hinsichtlich eigener Datennutzung, Sonderkonditionen, Organisationsform und möglicherweise bei Zusatzdiensten und wertsteigernder Datenanreicherung (bei DVMDs) sowie Erwerbszwecken (bei DAOs) macht es zumindest nicht einfacher, DVMDs und DAOs aufzubauen und Angebote zu schaffen, die Datenteilen und -spenden aktiv anreizen. Die grundsätzliche Logik, Datenteilen stärker voranzutreiben, besteht gleichwohl fort. Akteure der Datenökonomie sollten daher einerseits untersuchen, inwiefern DVMDs und anerkannte DAOs im Sinne des DGA dennoch ein gangbarer Weg für sie sind; andererseits aber auch aktiv prüfen, ob andere Konstruktionen, die nicht in den DGA fallen, für sie rechtlich möglich und wirtschaftlich-technisch sinnvoll sein könnten. Das könnte beispielsweise die Einrichtung eines gemeinnützigen, sektoralen Data Brokers sein, der keine direkten kommerziellen Beziehungen zwischen Datengebenden und Nutzenden herstellt – somit kein DVMD nach DGA ist und nicht unter die DGA-Bestimmungen fällt – aber dennoch so ausgestaltet wird, um möglichst hohes Vertrauen zu genießen (z. B. keine eigene Profitorientierung, Betrieb durch einen Branchenverband u.Ä.).

2.5.2. Data Act (DA)

Was sind die Ziele des Data Acts?
Das mit dem Data Act verfolgte übergeordnete Ziel ist die gerechtere Verteilung der Wertschöpfung aus Daten auf die Akteure im digitalen Umfeld. Datensilos sollen aufgebrochen und die dadurch freiwerdenden Daten für alle Akteure zugänglicher gemacht werden, sodass ein wettbewerbsorientierter Datenmarkt entsteht und neue Möglichkeiten für datengetriebene Innovationen geschaffen werden. Gleichzeitig sollen die Rechte derjenigen gestärkt werden, deren Produkte- und Dienstenutzung erst verwertbare Daten generieren.

Wie sollen diese Ziele erreicht werden?
Die Ziele des Data Acts sollen vor allem erreicht werden, indem Nutzer digitaler Produkte und darauf basierender Dienste mehr Kontrolle über die in ihren Produkten und den von ihnen genutzten Diensten anfallenden Daten erhalten. Als Nutzer gelten sowohl Privatpersonen als auch Unternehmen (Art. 2 Nr. 12) wie z. B. Anlagenbetreiber. So können Nutzer vom Dateninhaber die Bereitstellung von Daten – nach Möglichkeit in Echtzeit – für sich selbst oder für Datenempfänger verlangen (Art. 4 und 5). Dateninhaber sind alle natürlichen oder juristischen Personen, die Kontrolle über ein Produkt und einen damit verbundenen Dienst haben, und die dadurch in der Lage

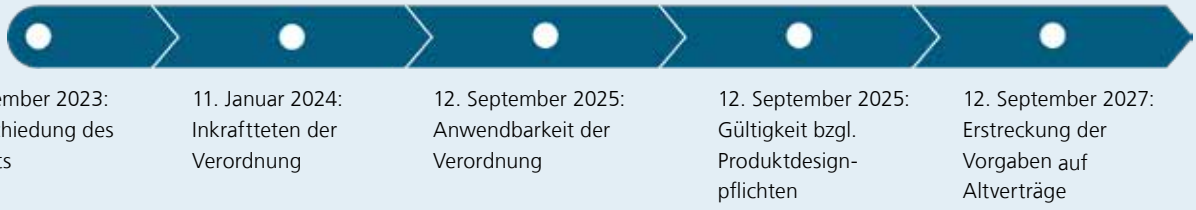


Abbildung 2: Schrittweise Auswirkungen des Data Acts
Der Data Act ist am 11. Januar 2024 in Kraft getreten, die meisten seiner Vorgaben erlangen allerdings erst 20 Monate nach Inkrafttreten Gültigkeit, also am 12. September 2025. Ausnahmen bilden die Pflichten aus Art. 3 Abs. 1, Produkte so zu gestalten, dass Daten standardmäßig für die Nutzer zugänglich sind, die ein Jahr später, also am 12. September 2026 Gültigkeit erlangen sowie die Erstreckung der Vorgaben auf Alt-Verträge, die erst ab dem 12. September 2027 Gültigkeit erlangen.

sind, Daten bereitzustellen (Art. 2 Nr. 13). Datenempfänger wiederum sind alle natürlichen oder juristischen Personen, denen zu geschäftlichen Zwecken auf Verlangen eines Nutzers Daten seitens des Dateninhabers bereitgestellt werden (Art. 2 Abs. 14).

Dateninhaber dürfen außerdem gemäß Art. 4 Abs. 13 durch den Nutzer generierte nicht-personenbezogene Daten nur noch dann selbst nutzen, wenn zuvor ein Vertrag mit dem Nutzer darüber geschlossen wurde. Art. 3 Abs. 2 und 3 verpflichten den Dateninhaber in diesem Zusammenhang zur Bereitstellung weitreichender vorvertraglicher Informationen gegenüber dem Nutzer. Auf diese Weise soll die Monetarisierung der Datennutzung vorangetrieben werden. Nutzer sollen die Wahl erhalten, ihre Daten entweder den Dateninhabern oder Datenempfängern bereitzustellen, je nachdem, wer ihnen den besseren Dienst anbietet oder mehr Entgelt für die Nutzung ihrer Daten anbietet.

Welche Daten sind vom Data Act umfasst?
Die Vorgaben des DA beziehen sich grundsätzlich einerseits auf Produktdaten (Art. 2 Nr. 15), die durch die Nutzung eines Produkts generiert werden, und andererseits auf verbundene Dienstdaten (Art. 2 Nr. 16), die die Digitalisierung der absichtlichen oder unabsichtlichen Interaktion des Nutzers mit dem Produkt darstellen. Allerdings beschränkt sich der Nutzerzugang ausschließlich auf »ohne Weiteres verfügbare Daten« (Art. 2 Nr. 17), die der Dateninhaber ohne unverhältnismäßigen Aufwand erhalten kann und wobei nicht über eine einfache Bearbeitung der Daten hinausgegangen wird. Umfasst sind also sowohl Rohdaten als auch sog. aufbereitete Daten (physikalische Größen wie Temperatur, Druck, Durchflussmenge, Position, Beschleunigung, Geschwindigkeit usw.) sowie die Metadaten (die den grundlegenden Kontext und Zeitstempel der Daten umfassen), die erforderlich sind, um die bereitgestellten Roh- und aufbereiteten Daten nutzbar zu machen (EG 15). Veredelte Daten, also insb. Analysen bzw. Interpretationen von Roh- oder aufbereiteten Daten, sind vom Nutzeranspruch auf Zugang und Weitergabe nicht umfasst. Darüber hinaus erstrecken sich die Regelungen des DA sowohl auf nicht-personenbezogene Daten als auch auf personenbezogene Daten. Die Vorgaben der DSGVO bleiben allerdings unberührt, d.h., dass Dateninhaber und -empfänger derzeit geltende Datenschutzregelungen auch weiterhin befolgen müssen.

Bestimmungen zur Datenübertragung vom Dateninhaber an den Datenempfänger
Weitere Bestimmungen regeln die Bedingungen der Datenübertragung vom Dateninhaber an den Datenempfänger. So sind die Daten zur Gewährleistung der Interoperabilität in einem strukturierten, gängigen, maschinenlesbaren Format bereitzustellen (Art. 5 Abs. 1). Außerdem können Dateninhaber gemäß Art. 9 vom Datenempfänger eine angemessene Gegenleistung für die Datenbereitstellung verlangen, müssen dabei allerdings verschiedene Faktoren (insb., wenn es sich bei Datenempfängern um KMUs handelt) berücksichtigen, um die Angemessenheit nachzuweisen.

Zudem ist es dem Datenempfänger gem. Art. 6 Abs. 2 lit. e insbesondere untersagt, die erhaltenen Daten für die Entwicklung eines Produktes zu nutzen, das mit dem Produkt im Wettbewerb steht, von dem die Daten stammen oder die Daten ihrerseits einem anderen Dritten zu diesem Zweck weiterzugeben. Auch Fragen des Schutzes von Geschäftsgeheimnissen werden geregelt (z. B. Art. 4 Abs. 6[7]).

Sonstige relevante Regelungen betreffen den Datenzugriff durch öffentliche Stellen unter außergewöhnlichen Umständen.

Was sind kritische Diskussionspunkte?
Kritische Diskussionspunkte betreffen insbesondere die Grenzziehung zwischen bereitzustellenden Roh- und aufbereiteten Daten sowie veredelten Daten, die nicht unter das Gesetz fallen. Seitens der europäischen Wirtschaft wird befürchtet, dass rechtliche Unklarheiten zum Abfluss von Geschäftsgeheimnissen an die außereuropäische Konkurrenz führen könnten. Seitens der europäischen Energiewirtschaft wird auch befürchtet, dass der DA in einer aus ihrer Perspektive ohnehin bereits unübersichtlichen Regulierungslandschaft zu mehr Rechtsunsicherheit führen könne. Die von der EU-Kommission in Folge des Digital Markets Acts als »Torwächter« definierten Akteure (aktuell sieben Unternehmen, darunter (Alphabet [Google], Amazon, Apple, ByteDance [TikTok], Meta [Facebook, Instagram, WhatsApp], Microsoft und Samsung) sind aufgrund ihrer marktbeherrschenden Stellung von den Regelungen des Data Acts ausgeschlossen. Dadurch soll ein Datenabfluss zumindest an die größten Digital-Player verhindert wird.

Fraglich ist auch, wie die umfassenden Regeln des Data Acts in der Praxis durchgesetzt werden sollen: So ist zwar die Nutzung von bereitgestellten Daten zur Entwicklung eines Konkurrenz-Produkts untersagt, ob sich Datenempfänger an dieses Verbot halten und wie es im Zweifel zu kontrollieren wäre, ist noch offen.

2.6. Exkurs: Mögliche Geschäftsmodelle für Datentreuhänder

Aktuell laufen zahlreiche Versuche, um tragfähige **Geschäftsmodelle** für Datentreuhänder (DTH) zu etablieren. Ein

7 Regulation (EU) 2023/2854 - Data Act verfügbar unter https://eur-lex.europa.eu/eli/reg/2023/2854

definitives Modell hat sich jedoch noch nicht herauskristallisiert. Aufgrund der Heterogenität der Branchen und Anwendungsfeldern ist zu vermuten, dass sich unterschiedliche branchenspezifische Modelle entwickeln werden. Gleichwohl wird jedes belastbare Geschäftsmodell drei Kernfragen beantworten müssen:

- Welches Wertversprechen bietet der Datentreuhänder den Datennutzenden und Datengebenden?
- Wie finanziert sich der Datentreuhänder?
- Werden Gewinnabsichten verfolgt?

Datentreuhänder können grundsätzlich **Gewinnabsichten** verfolgen. Zwei Gründe können jedoch für eine non-profit-Orientierung sprechen: Erstens kann es für einen non-profit-DTH einfacher sein, Vertrauen aufzubauen, v. a. wenn der Betreiber auch eine den Branchenakteuren bekannte, neutrale Größe ist (z. B. ein Verband oder ein Konsortium). Zweitens ist es für einen primär nur auf Kostendeckung wirtschaftenden DTH tendenziell leichter, die Kosten (z. B. Gebühren) für Datengebende und -nutzende niedrig zu halten, was Hürden für eine Teilnahme ihrerseits senkt.

Bestehende DTHs scheinen oft zumindest einen Teil ihrer **Finanzierung** aus staatlichen oder privaten Zuwendungen (z. B. Verbände, Stiftungen, Firmenkonsortien) zu beziehen. Ferner werden oft Gebühren von Datennutzenden (seltener von Datengebenden) erhoben, oder sind zumindest geplant. Hier gibt es viele Möglichkeiten: Gebühren können z. B. als Subskriptionsmodell (Zeitperiode, Datenvolumen) oder nach Zugriff strukturiert, eine Freemium-Komponente enthalten (bis zu einem Schwellwert kostenlos, dann Gebührenpflichtig), oder nach Nutzenden gestaffelt werden z. B. verbilligte Zugriffe für KMU oder Universitäten (Kreutzer 2023). Je nach Branchenkontext können individuellere Modelle sinnvoll sein. Im medizinischen Bereich ist es z. B. üblich, dass Pharmakonzerne die oft achtstelligen Kosten für Datenbestandsergänzungen von Biobanken tragen und dafür eine temporäre Exklusivnutzung dieser Daten bekommen, bevor sie für alle freigegeben werden.[8]

Das **Wertversprechen** bestimmt, welche Dienste der DTH anbietet. Kerndienstleistung wird in der Regel sein, **Datenaustausche** zu ermöglichen. Hier sind zwei grundlegende rechtlich-organisatorische Spielarten möglich. Die erste ist, dass der DTH *direkte* Datenaustausche zwischen den Gebenden und Nehmenden ermöglicht, die als *direkte Geschäftsbeziehungen zwischen diesen zwei Parteien* strukturiert werden. In dem Fall fällt der DTH in den Geltungsbereich des DGA. Das hat den Vorteil, dass der DTH sich als »anerkannten DVMD« registrieren lassen kann, was vertrauensfördernd sein kann. Es erlaubt auch, die Datenaustausche technisch als direkte Datenflüsse zwischen Gebenden und Nehmenden zu strukturieren – d.h., ohne dass Daten über den DTH selbst fließen. Dies dürfte die sicherheitstechnischen wie Compliance-bezogenen Anforderungen und Kosten für den DTH reduzieren. Gleichzeitig ist der DTH dann allen Anforderungen und Einschränkungen des DGA unterworfen.

Alternativ kann der **Datenaustausch** auch als *Geschäftsbeziehungen jeweils nur zwischen dem DTH und dem Datengebenden bzw. Nutzenden* strukturiert werden, *ohne* direkte Beziehungen zwischen Gebenden und Nutzenden. Damit würde der DTH aus dem DGA herausfallen, was regulatorische Freiräume schafft. Der Datenfluss würde dann aber vermutlich in jedem Fall über den DTH laufen und die Daten – möglicherweise längerfristig – in der direkten Obhut des DTH sein – mit allen zusätzlichen sicherheitstechnischen und rechtlichen Anforderungen, aber potenziell auch der Möglichkeit, zusätzliche Angebote und Wertversprechen für Gebende und Nutzende zu entwickeln. Je nach Branchen- und Anwendungskontext könnten sich auch Zwischenformen, die unterschiedliche Elemente dieser beiden rechtlich-organisatorischen Grundformen eines DTH vereinen, anbieten.

Wichtige Teile dieser Kerndienstleistung »Datenaustausch« (egal wie sie strukturiert ist) dürften regelmäßig die Folgenden sein:

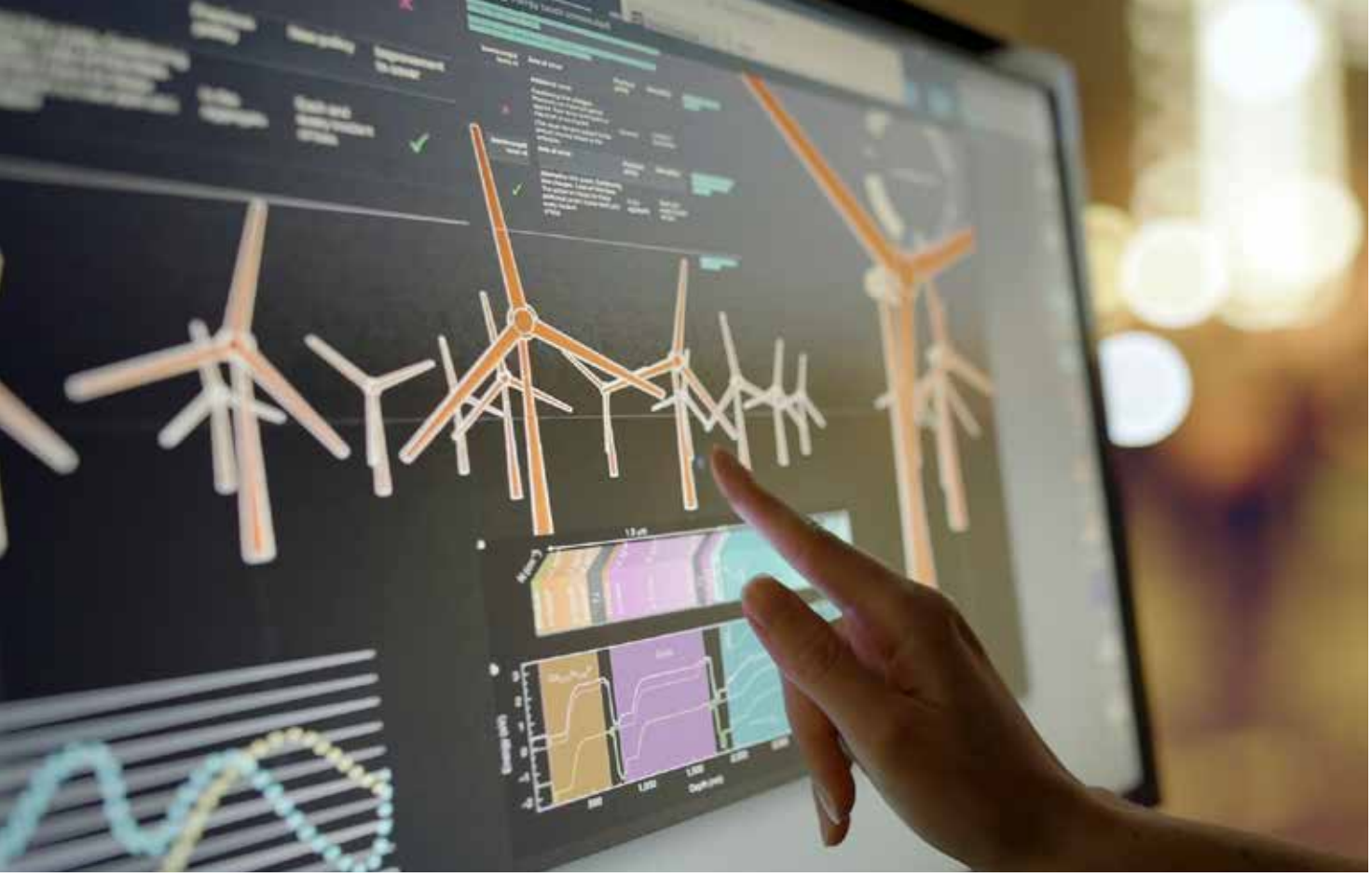
- Bereitstellung der nötigen technischen Infrastruktur für den Datenaustausch, einschließlich einer technisch-organisatorischen Architektur, die es den Datengebenden einfach macht, Einblick in die Nutzung ihrer Daten zu nehmen (Zwecke, Verfahren, eventuell Ergebnisse) und eine Datensouveränität darüber auszuüben (d.h. Nutzungen untersagen und Daten löschen zu können).
- Gewährleistung von Datensicherheit und Datenschutz, die Einhaltung der Nutzungs- und Austauschvereinbarungen sowie sonstiger Compliance seitens der Gebenden/Nutzenden, ggf. Unterstützung der Parteien dabei.
- Sicherung der Qualität der Daten und Metadaten.
- Weitere Aufbereitungen der Daten, die vor allem dazu dienen, den Datenaustausch zu ermöglichen oder erleichtern: Anonymisierung oder Pseudonymisierung, Formatierung, eventuell Bereinigungen.

Um diesen »Kern« herum können weitere Dienstleistungen gestaltet werden. Eine potenziell sehr wichtige Dienstleistung ist, als **»Matchmaker«** und sogar **Use Case-»Orchestrator«** für Datengebende und Nutzende zu fungieren. Wie oben

8 Hierzu weiter Kreutzer, S. et al. (2023): Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Bericht zu Arbeitspaket 1.2: Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle. Technopolis Group

erläutert, erfordert die Identifikation und Entwicklung neuer Use Cases oft intensive Kommunikation zwischen Gebenden und Nutzenden sowie vertieftes Verständnis ihrer jeweiligen Domänen und sogar Geschäftsmodelle und technischen wie geschäftlichen Fähigkeiten. Ohne dieses kann es schwierig sein, überhaupt zu erkennen, welche Daten, Partner und möglichen neuen Anwendungen interessant sein könnten. Wenn Datentreuhänder ein vertieftes Wissen über ihre Teilnehmer und deren Daten und Domänen aufbauen, können sie gezielt potenzielle Gebende/Nutzende zusammenbringen und diese Gespräche und Identifikations-/Entwicklungsprozesse orchestrieren.

Derartige Matchmaking- oder sogar Company-/Use-Case-Builder-Dienste sollten auch unter dem DGA rechtlich unproblematisch sein, da der DTH (DVMD) dabei die Daten des Gebenden nicht selbst nutzt (zumindest nicht zu Zwecken, die über die Ermöglichung des Datenaustauschs hinausgehen). Es sind aber auch **Zusatzdienste** denkbar, die auf der Verarbeitung bereitgestellter Daten basieren. Diese könnten für Gebende wie Nutzende ebenfalls sehr interessant sein, wären aber möglicherweise rechtlich schwieriger für einen DTH, der unter den DGA fällt. Gleichwohl befindet sich die Rechtsauslegung hier noch im Fluss. Eine Rechtsprüfung wäre in jedem Fall ratsam. Zu solchen Diensten zählen potenziell z. B. die Anreicherung von Daten mit zusätzlichen Informationen und/oder ihre Aggregierung zu größeren Datenprodukten, sowie das Angebot von Analytics-Werkzeugen und/oder Dienstleistungen sowie sonstige eigene Auswertungen der Daten.



3. Anwendungsbeispiele für Datenaustausch in der Energiewirtschaft

3.1. Datenspende und Treuhand für HEMS-Daten

Die Fahrpläne der Stromversorger basieren in weiten Teilen auf Standard-Lastprofilen des Verbrauchs von Haushalten. Die tatsächlichen Lastprofile weichen jedoch zunehmend von diesen Standard-Lastprofilen ab. Dadurch entstehen Mehrkosten in der Stromversorgung, weil die Prognosefehler kurzfristig durch teure Ausgleichsenergie ausgeglichen werden. Um die zukünftigen Realitäten im Stromverbrauchsverhalten abbilden zu können, sind umfangreiche und detaillierte Daten von Haushalten, ggf. ergänzt um Informationen zu deren Ausstattung mit PV-Anlagen, Heimspeichern, Wärmepumpen, Wallboxen oder Home Energy Management-Systemen erforderlich.

Der Data Governance Act gibt jetzt privaten und gewerblichen Verbrauchern die Möglichkeit, ihre Verbrauchsdaten in hoher zeitlicher Auflösung an Datentreuhänder (Datenvermittlungsdienste) und Data Altruism Organisations weiterzugeben. Diese bieten Möglichkeiten, um die Daten für zusätzliche Nutzungen und Anwendungen durch Stromlieferanten, Netzbetreiber und weitere Akteure im Energiesystem (z. B. Forschungsinstitute) zweckgebunden zur Verfügung zu stellen. Dabei wird der DTH bzw. die DAO zwischen die datengebenden Haushalte und die datennutzenden Stromversorger u. a. »zwischengeschaltet« und regelt den Datenzugriff und ggf. weitere Aspekte der Data Governance. Hier gibt es verschiedene Ausgestaltungsoptionen:

- DTH/DAO als datenverarbeitende und speichernde Stelle: Daten können vom Treuhänder bzw. der DAO erhoben, bei sich gespeichert und dann den Datennutzern zur Verfügung gestellt werden.
- DTH/DAO ohne eigenen direkten Zugriff auf die Daten: Alternativ können DTH/DAO den Datenaustausch zwischen

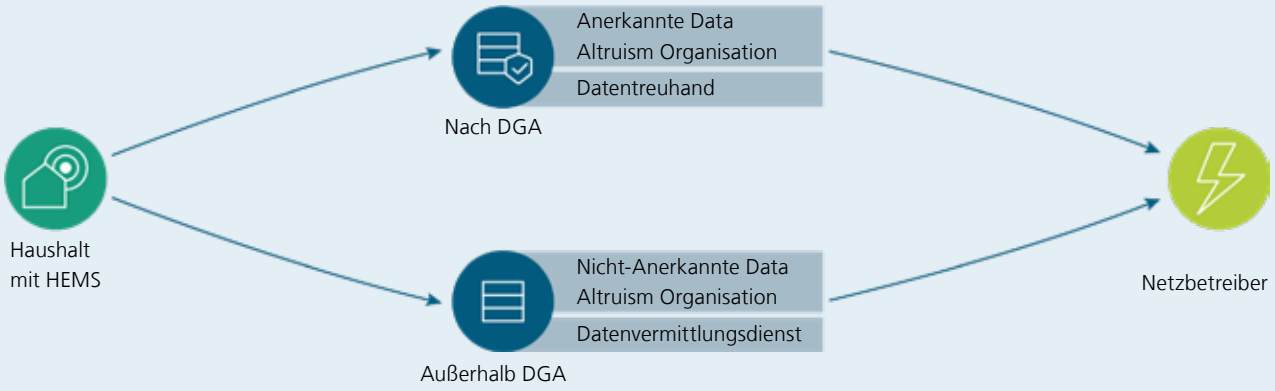


Abbildung 3: Datenspende zum Stromverbrauch aus HEMS zur Ermittlung von Lastprofilen innerhalb und außerhalb des Data Governance Act (DGA)

den Haushalten und den Datennutzenden regeln und überwachen, ohne eigenen direkten Zugriff auf die Daten.

Für die konkrete Organisationsform der Datentreuhänder und DAOs gibt es ebenfalls verschiedene Ausgestaltungsoptionen:

- Datentreuhänder als Datenvermittlungsdienst (DVMD) im Sinne des DGA,
- Datentreuhänder, der eine Organisationsform wählt, die nicht unter die Regeln des DGA fällt.

Die Optionen – DTH außerhalb des DGA, DVMD unter dem DGA, »anerkannte« DAO unter dem DGA, nicht-anerkannte außerhalb – haben Vor- und Nachteile, die je nach Anwendungsfall unterschiedlich ausfallen. Eine DAO könnte gerade für Haushalte die »vertrauenerweckendste« Form sein; da zumindest eine »DGA-anerkannte« DAO aber den Datenspendern keine direkten monetären Vorteile bieten darf, könnte es ihr schwerfallen, ausreichend Anreize für Spender zu schaffen. Der Nutzen für die Spender entstünde sehr indirekt und mittelbar über niedrigere Netzentgelte für alle Stromkunden.

Wie besprochen genießt ein DTH außerhalb des DGA größere Freiheiten hinsichtlich Geschäftsmodellen und Datennutzungen als ein DVMD im Sinne des DGA, die es einfacher machen können, Nutzenden und Gebenden Mehrwerte zu stiften. Um dem DGA zu »entkommen» könnten allerdings Organisationsstrukturen nötig werden, die selbst neue Kosten verursachen, während etwaige Vertrauensvorteile durch ein Branding als »Anerkannter DVMD» verloren gehen. Kurz: Die jeweiligen Vor- und Nachteile müssen genau analysiert und abgewogen werden, ein konkreter möglicher Nutzen aus den Daten ist aber klar erkennbar.

3.2. Datenaustausch beim Betrieb von Windenergieanlagen

Moderne Windenergieanlagen sind komplexe Maschinen, deren Funktion über mit mehreren Hundert Sensoren geregelt und überwacht wird. Die von diesen Sensoren erzeugten Daten sind zentral für den Betrieb der Anlagen aber auch für die vorausschauende und reaktive Wartung und Instandsetzung. Der Zugang und die Nutzung zu diesen Daten werden in der Regel über den Kaufvertrag zwischen Hersteller und Betreiber geregelt. Dabei erwirbt der Käufer meist eine Teilmenge der verfügbaren Daten. Der Hersteller erhebt die volle Datenmenge in eigenen Systemen.

Gleichzeitig werden häufig mit dem Kauf auch langjährige Vollwartungsverträge abgeschlossen, die die Verantwortung für den Service auf den Hersteller, bzw. dessen Servicepartner übertragen und dem Betreiber eine Mindest-Verfügbarkeit zusichert. Durch die exklusive Datenverfügbarkeit hat der Hersteller-Service dabei einen Wettbewerbsvorteil gegenüber unabhängigen Service-Dienstleistern.Durch den Data Act wird es für Betreiber künftig erweiterten Zugang zu Daten und klare Nutzungsrechte an diesen Daten ihrer Anlagen geben. Dadurch können Daten gemeinsam mit Dritten, die nicht im Wettbewerb zum Hersteller stehen, genutzt werden. Vorstellbar ist hier die Einbindung von externen Software-Services etwa zur Fehlerfrüherkennung. Auch eine Zusammenarbeit mit Zulieferern beim Zustandsmonitoring oder anderen Diensten zu einzelnen Komponenten wird möglich. Nutzungen der Daten sind auch im nicht-technischen Bereich bei der Bewertung von Ausfall- oder Schadensrisiken für Finanzierer und Versicherungen potenziell relevant.

3.3. Datenaustausch zur Nutzung von Daten aus Elektrofahrzeugbatterien

Das Ladeverhalten der schnell steigenden Zahl von E-Fahrzeugen hat zunehmende Relevanz für das Stromsystem. So muss der Strombedarf für das Laden der Fahrzeuge möglichst genau vorhergesagt und eingeplant werden. Hohe, gleichzeitige Ladeleistungen können zudem zu Engpässen im Verteilnetz führen. Deshalb sind auch örtlich-zeitliche Vorhersagen nützlich. Außerdem ist im Fahrzeugbestand insgesamt ein großer Batteriespeicher räumlich verfügbar, der zukünftig insbesondere durch bidirektionales Laden eine wichtige Quelle für Flexibilität im Stromnetz sein wird.

Für alle diese Funktionen ist der Zugang zu Batteriedaten der Fahrzeuge erforderlich. Diese umfassen die Nennleistung und -kapazität der Batterie, den aktuellen Ladestand, den technischen Zustand der Batterie und die möglichen Betriebspunkte. Diese Daten sind Teil des Batteriemanagement-Systems und liegen im Fahrzeug und bei den Herstellern vor. Die Fahrzeug-Batterien sind in E-Fahrzeugen die Komponenten mit dem höchsten Wertanteil. Die Batterieeigenschaften und das Batterie-Management gelten als zentrales Know-how für Hersteller in der E-Mobilität. Deshalb sind Hersteller sehr zurückhaltend, diese Daten herauszugeben, da sie Nachteile durch die Kombination und das Re-Engineering von Steuerungs-Know-how aus den Daten vermeiden wollen.

Mit dem Data Act erhalten Autokunden ein Recht auf den Zugang zu ihren Batteriedaten und dürfen diese auch an Dritte weitergeben. Auch aus der EU-Erneuerbare-Energien-Richtlinie (RED) III heraus sollen Batteriedaten aus Heimspeichern und E-Fahrzeugen für Anwendungen im Energiesystem bereitgestellt werden.

Der Interessenkonflikt zwischen energiewirtschaftlicher Nutzung und dem Schutz sensibler IP der Hersteller kann durch den Einsatz eines Datentreuhänders aufgelöst werden, ob als DVMD im Sinne des DGA oder anderweitig organisiert. Unter Umständen könnte sich auch eine DAO anbieten, wobei die wirtschaftlichen Interessen der Beteiligten wie das Problem der Beanreizung der Fahrzeugbesitzer dem entgegenstehen könnten. Der Treuhänder würde den Austausch der Daten zwischen den Akteuren regeln und ihre zweckbezogene Nutzung für energiewirtschaftliche Anwendungen garantieren. Dabei könnte der Datenfluss entweder über den DTH stattfinden (»man in the middle«), oder direkt zwischen den Gebenden und Nutzenden. In jedem Fall würde der DTH den Zugang zu den Daten und die Einhaltung der Nutzungsbedingungen kontrollieren, die Daten pseudonymisieren und ggf. aggregieren, sowie sicher verschlüsseln. Schließlich würde er voraussichtlich Aspekte der Compliance und Verwaltung für die Beteiligten abwickeln und eventuell als Matchmaker auftreten.

Das Vertrauen in und die Akzeptanz für die Organisation des Datentreuhänders spielt angesichts der Größe der beteiligten Akteure und der Intensität der Interessenslagen eine wichtige Rolle, zumal in diesem Feld der Sektorenkopplung auch kein klarer Branchenverband für diese Funktion prädestiniert wäre. Alternativ dazu kann eine Lösung regulatorisch diskutiert und geschaffen werden.

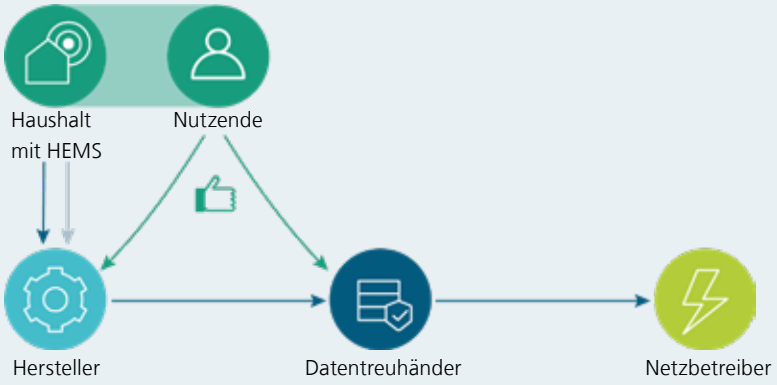


Abbildung 4: Derzeitiger und zukünftiger Datenfluss von HEMS-Daten über einen Datentreuhänder an Netzbetreiber
Quelle: eigene Darstellung

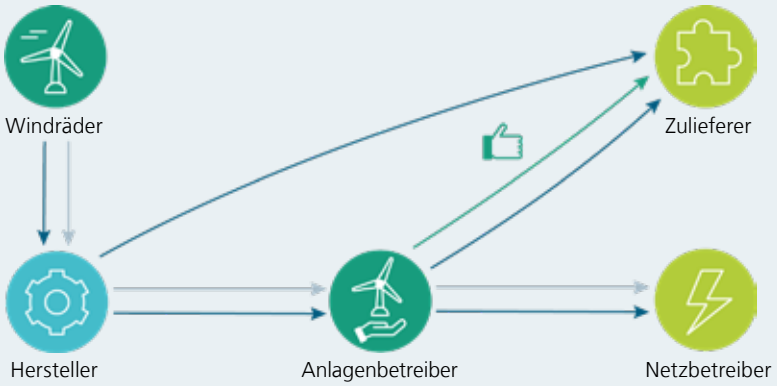


Abbildung 5: Derzeitiger und zukünftiger Datenfluss von Windanlagen-Daten an dritte Serviceanbieter. Quelle: eigene Darstellung

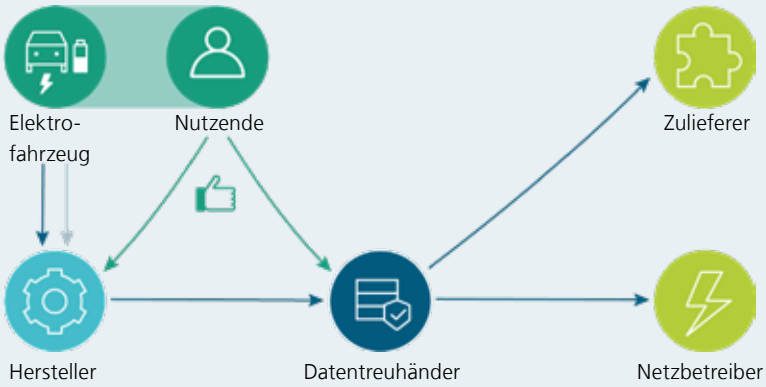
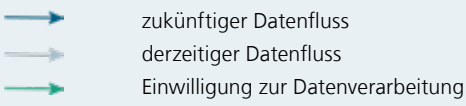


Abbildung 6: Derzeitiger und zukünftiger Datenfluss von Daten aus Elektrofahrzeugbatterien über einen Datentreuhänder an Netzbetreiber und dritte Serviceanbieter
Quelle: eigene Darstellung



4. Chancen und Handlungsoptionen

4.1. Chancen für den Datenaustausch durch Data Act und Data Governance Act

Anwendungsbereiche
Die Anwendungsbeispiele zeigen, dass durch die neuen Regulierungen zur Datennutzung per Data Act und Data Governance Act Chancen für eine verbesserte Datennutzung entstehen und technische Lösungen und Umsetzungen für Industrieakteure einfacher werden können. Dafür ist es notwendig, ausreichende Anreize für potenzielle Teilnehmer zu schaffen.

Data Act
Die zukünftigen Nutzungsrechte an den Daten aus eigenen Anlagen durch den Data Act eröffnet eine Vielzahl von Möglichkeiten. Aus energiewirtschaftlicher Sicht besteht ein besonderes Interesse an den HEMS-Systemen. Aus diesen Daten lassen sich Informationen generieren, die etwa Netzbetreiber und Stromlieferanten zur Optimierung ihrer Prozesse nutzen können. Das kann durch bessere und individuellere Lastprofile und Lastprognose oder die Bereitstellung von Flexibilität für den Strommarkt oder im Engpassmanagement sein. Hier kann ein großes Potenzial digital adressierbar und vermarktbarer Flexibilität erschlossen werden (European Commission 2022).

Zudem profitieren alle Betreiber der Anlagen im Energiesystem von der Nutzbarkeit ihrer Betriebsdaten. Daraus lassen sich die allgemein diskutierten Vorteile zur Optimierung von Betrieb und Instandhaltung auch für den Energiesektor nutzen. Dies ist vor dem Hintergrund der hohen Kapitalintensität der Erneuerbare-Energie-Anlagen eine wichtige wirtschaftliche Verbesserung.

Bedeutsam für die Mobilisierung der Potentiale wird die Nutzbarkeit der Daten in einem klar verständlichen Format,

möglichst unter Verwendung einschlägiger technischer Standards sein. Ein weiteres Erfolgskriterium ist die Bereitstellung gut dokumentierter Schnittstellen (z. B. REST-API), damit die Daten einfach und automatisierbar in weitere Systeme eingebunden werden können. Der Zugang zu diesen Schnittstellen erfordert dann Autorisierungskonzepte und Authentifizierungsverfahren, um den berechtigten Datenzugang sicher zu gestalten. Hier können die Konzepte der Datenräume Ansätze für die Zugangskontrolle auf Basis gemeinsamer Identitätskonzepte liefern.

Data Governance Act

Die durch den Data Governance Act rechtlich konkretisierten Modelle zur Datenspende und zu Datenvermittlungsdiensten (Datentreuhandmodellen) können dazu beitragen, Interessenskonflikte oder Motivationsbarrieren bei der Nutzung von Daten aufzulösen. Gleichzeitig bedarf es an Anreizen für potenzielle Teilnehmer, sich an diesen Modellen zu beteiligen. Außerdem können sich Datentreuhänder auf den Abschluss von Datennutzungsvereinbarungen mit Datengebern und -nehmern spezialisieren und dadurch die Prozesse effizient gestalten. Daraus resultiert die Chance, dass Vereinbarungen und Verhandlungen einfacher geführt werden können und klarere Rechtsgrundlagen für die Nutzung von Daten entstehen. Die Reduzierung rechtlicher Risiken kann auch den Zugang für kleinere Akteure erleichtern.

Eine wichtige Frage dabei ist, wer Betreiber eines Datentreuhänders, einer Datenspende-Gesellschaft oder eines Datenraums als Datenvermittlungsdienst sein können. Die Organisationen, die diese Rolle einnehmen, sollen das Vertrauen in den Datennutzungsprozess von Organisationen stärken, die nicht direkt miteinander eine Datennutzung vereinbaren wollen. Entscheidend ist deshalb, welche Probleme es in der Branche gibt, die über DTHs oder Datenspende-Modelle gelöst werden können. Insofern müssen diese Organisationen hohen Anforderungen zur technischen und organisatorischen Integrität genügen und im besten Fall bereits das Vertrauen der Geschäftspartner im Markt haben. Zu klären wäre deshalb, ob bzw. welche Rolle Verbände in der Datenökonomie spielen können, indem sie z. B. DTHs anbieten.

Wegen der bisher schwierigen Gestaltung der Geschäftsmodelle für diese Rollen ist eine mögliche Perspektive, dass sich eine geringe Zahl von domänenspezifischen Datenspezialisten herausbildet, die zum Teil komplexen Anforderungen im

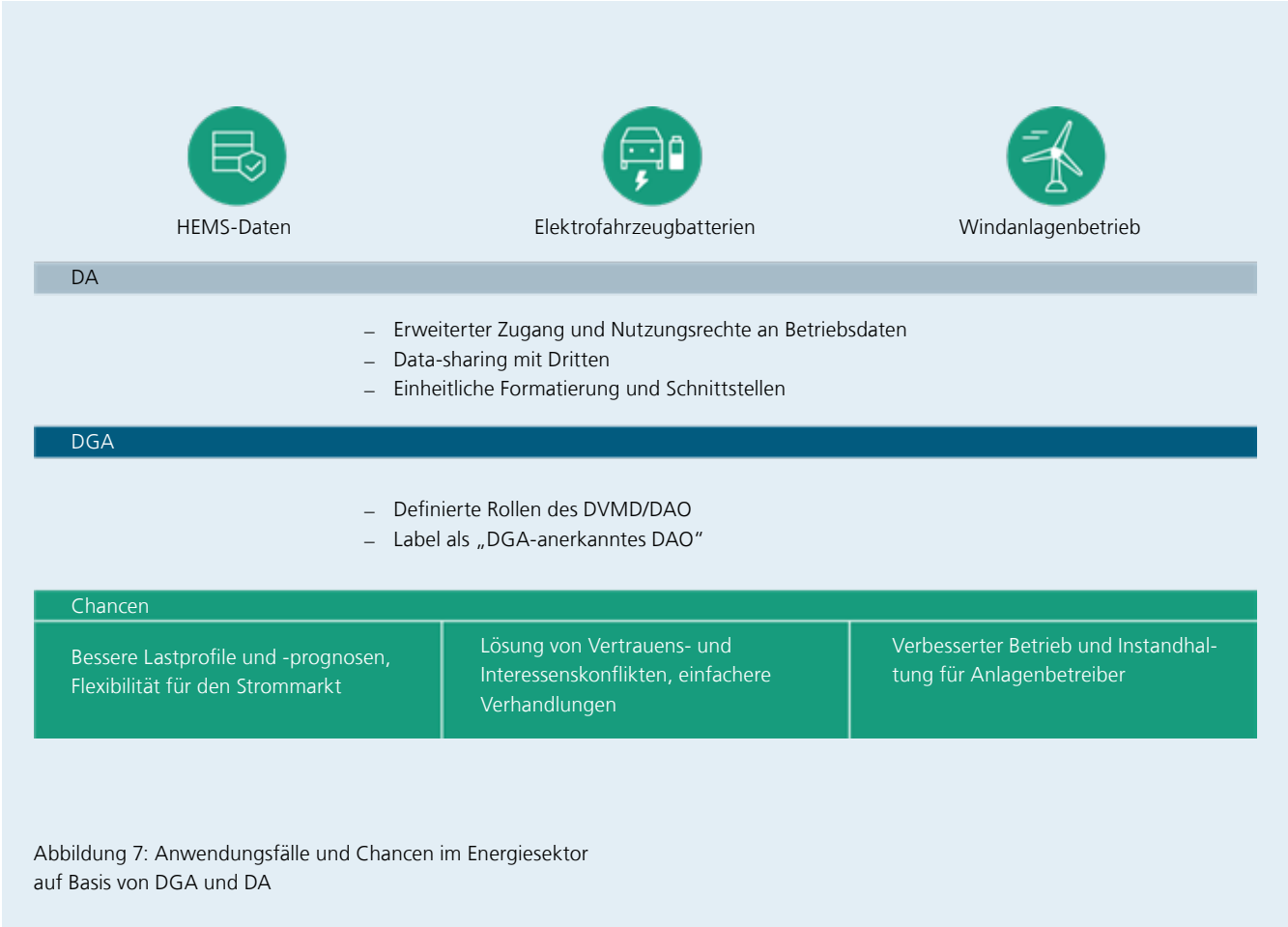


Abbildung 7: Anwendungsfälle und Chancen im Energiesektor auf Basis von DGA und DA

Bereich Technologie und Compliance erfüllen, Dienstleistungen zur Verfügung stellen und Beratungsdienste zur Nutzung der Dateninfrastruktur anbieten.

4.2. Herausforderungen und Implikationen

Data Act
Während für Anlagenbetreiber neue Rechte aus dem Data Act erwachsen, verlangt der Data Act insbesondere von den Unternehmen im Anlagen- und Maschinenbau, sich den kommenden Verpflichtungen bewusst zu sein und diese durch die Entwicklung von digitalen Angeboten zu erfüllen. Dies sollte mit der Entwicklung einer Strategie einhergehen, wie die neuen Kundenbeziehungen für das zukünftige Geschäft genutzt werden können. Insofern entsteht sowohl Umsetzungsaufwand als auch Risko für das zukünftige, datenbasierte Geschäft für diesen Sektor.

Data Governance Act
Für unternehmerische Entscheidungen für oder wider die Teilnahme an Datentreuhandmodellen oder Datenvermittlungsdiensten ist eine belastbare, mittelfristige Perspektive notwendig. Während der Nutzen der Teilnahme gerade am Anfang eines Modells noch unsicher ist, zum Teil auf Netzwerkeffekten beruht und damit häufig erst durch die Teilnahme einer kritischen Masse weiterer Akteure entsteht, kann die Motivation auf individueller Organisationsebene fehlen.

Hinzu kommt, dass die umfangreichen Anforderungen zu hohen Kosten bei Datentreuhändern und -vermittlungsdiensten führen, die über das Geschäftsmodell auf die Teilnehmer umgelegt werden müssen. Hinzu kommt ein rechtliches Risiko, das sich ebenfalls auf die Kosten und auf die Anzahl der Anbieter auswirken kann.

Unternehmen und Verbände sollten in dieser Situation prüfen, ob sich durch einen DTH oder DVMD werthaltige Anwendungsfälle umsetzen lassen oder rechtliche Verpflichtungen kollaborativ gelöst werden können. Zur Umsetzung sind im nächsten Schritt finanziell tragfähige Modelle zu entwickeln, dabei sollten auch Chancen einer Broker-Rolle betrachtet werden. Das ausgewählte Konzept muss Anreize für alle beteiligten Akteure enthalten. Zur Umsetzung können mithilfe öffentlicher Förderung Leuchtturmprojekte finanziert und damit ein wichtiger Teil der Entwicklungskosten am Anfang finanziert werden. Mittelfristig sollten sich derartige Projekte mit weiteren Domänen vernetzen. Im Hinblick darauf ist die Anwendung von Standards bei Daten, Prozessen und Ökosystemen von hoher Bedeutung.

Politik
Auf dem Weg zur Umsetzung der im DGA vorgesehenen Funktionen und Dienstleistungen besteht ein Trilemma, wegen hoher Unsicherheiten, geringer Motivation der Akteure und hohen Kosten der Umsetzung. Diese Herausforderung hemmen die Entwicklung in einem Bereich, der eigentlich die Reibung im System auflösen soll.

Auch die explizite Beschränkung des Leistungsspektrums eines Datenvermittlungsdienst im Sinne des DGA, der keine eigene kommerzielle Verwendung der der Daten erlaubt, erschwert die Entwicklung von tragfähigen Geschäftsmodellen. In der Kundenbeziehung kann das dazu führen, dass Akteure zusätzliche Leistungen beim DTH zwar nachfragen, aber nicht bekommen dürfen. Unsicher ist darüber hinaus, inwiefern tatsächlich Nutzen durch die vorgesehenen Label entstehen.

Wichtig ist es aus politischer Sicht nun, Rechtssicherheit für die zum Teil noch unbestimmten und neuen Regelungen des DGA zu schaffen. Gleichsam sollte diese Auslegung weite Spielräume bei der Ausgestaltung und Auslegung lassen, damit im geltenden Rahmen unterschiedliche Ansätze erprobt werden können.

Dafür ist während der Anlaufphase weiterhin eine Förderung von Experimenten mit den für die Anwendungsfälle relevantesten Akteuren sinnvoll. Diese sollten sowohl im For-profit- als auch im Non-profit-Sektor angesiedelt sein. Wegen ihrer zentralen Rolle sollten ebenfalls Initiativen zur Datenstandardisierung und zur Pflege von Datenmodellen und deren Transfer in die Anwendung gefördert werden.

Industrie
Um die in diesem Whitepaper beschriebenen Anwendungsbeispiele und weitere Anwendungen zu realisieren, ist ein Zusammenspiel der individuellen Motivation der teilnehmenden Akteure, der Technologie und der rechtlichen Rahmenbedingungen erforderlich.

Zentral ist dabei eine klare Motivation für die Teilnehmer. Der subjektive Nutzen einer Teilnahme an einem Modell muss die Kosten überwiegen und dies innerhalb eines überschaubaren Zeitraums bei der Entscheidungssituation. Es muss zudem klar sein und klar kommuniziert werden, woher für Dateninhaber der Anreiz kommt, ihre Daten weiterzugeben. Hier besteht zum Teil ein Vermittlungsproblem und zum Teil ein Interessenskonflikt für Akteure, die ihr Geschäftsmodell auf einem Datenvorsprung aufbauen.

Als weitere Grundlage muss das Thema Vertrauen in die beteiligten Organisationen und Technologien noch besser verstanden bzw. noch komplexer gedacht werden. Der Ansatz der Regulierung, insbesondere im Data Governance Act über eine Zertifizierung von Akteuren Vertrauen zu schaffen, adressiert einen zentralen Punkt beim Aufbau einer fairen Datenökonomie. Die Zertifizierung allein ist jedoch nicht ausreichend, um Vertrauen für einen stärkeren Datenaustausch zwischen

Akteuren zu schaffen. Für die Akteure ist der eigene Nutzen an einem stärkeren Datenaustausch sowie ein fairer Interessenausgleich zwischen beteiligten Akteuren von zentraler Bedeutung, der durch die Zertifizierung allein nicht gelöst wird. Eine weitere notwendige Bedingung, um Vertrauen herzustellen ist eine sichere Technologie, mit welcher der Zugang zu den bereitgestellten Daten kontrolliert werden kann. Dadurch wissen die Dateninhaber, welche Akteure Daten verwenden und verwerten.

Für die Unternehmen der Branche ergibt sich insbesondere die Aufgabe, sich die Verpflichtungen und Chancen bewusst zu machen und eigene Daten- und Digitalstrategien zu entwickeln. Unternehmen in der Rolle als Dateninhaber müssen insbesondere die technischen Grundlagen zum Datenzugang schaffen und die verpflichtenden vorvertraglichen Informationen rechtlich vorbereiten. Auf Branchenebene sollte das Thema in den Verbänden und Standardisierungsgremien präsent sein und weiterverfolgt werden.

Auf politischer Ebene erfüllen sich die Erwartungen der EU bisher nicht. Offene Rechtsfragen hemmen die Entwicklung, komplexe Anforderungen erschweren die Umsetzung von Geschäftsmodellen für Datentreuhänder. Damit ist der DGA in Teilen über das Ziel hinausgeschossen. Hier sollte politisch und regulatorisch nachgebessert werden.

Trotz dieser Unzulänglichkeiten bergen die neuen Regelungen enorme Chancen für die Datenwirtschaft im Energiesektor. Diese sollten auf Branchenebene mit den Verbänden oder anderen Brancheninitiativen weiter in Projekten konkretisiert, gefördert und umgesetzt werden.

5. Abbildungsverzeichnis

6. Literaturverzeichnis

Bitkom (2023): Presseinformation: Data Act: Bitkom-Präsident Wintergerst zum Abschluss der Trilog-Verhandlungen.
Online verfügbar unter https://www.bitkom.org/Presse/Presseinformation/Data-Act-Bitkom-zum-Abschluss-Trilog-Verhandlungen, zuletzt geprüft am 12.07.2024.

Bitkom (2023b) Bitkom Umfrage https://www.bitkom.org/Presse/Presseinformation/Datenoekonomie-Unternehmen-nutzen-Daten#

Digitaleurope (2023): Joint Statement: The Data Act is a leap into the unknown. Online verfügbar unter https://www.digitaleurope.org/news/joint-statement-the-data-act-is-a-leap-into-the-unknown/, zuletzt geprüft am 12.07.2024.

Eurelectric (2022): Commission proposal for a Data Act - A Eurelectric position paper. Online verfügbar unter https://cdn.eurelectric.org/media/5911/eurelectric-data-act-position-paper_final-h-E8583728.pdf, zuletzt geprüft am 12.07.2024.

European Commission (2022); Directorate-General for Energy; Klobasa, M.; Kühnbach, M.; Singh, M.; Knorr, K.; Schütt, J.; Boer, J.; Rolser, O.; Hernandez Diaz, D.; Fitzschen, F.; Garcerán, A.; Reina, R.; Stemmer, S.; Steinbach, J.; Popovski, E.; Antretter, M. : Digitalisation of energy flexibility. https://doi.org/10.2833/113770.

European Commission (2024): Data Governance Act explained. Online verfügbar unter https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained, zuletzt geprüft am 12.07.2024.

Kerber, W. (2021): DGA - einige Bemerkungen aus ökonomischer Sicht, https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf Kreutzer, S.; Heimer, T.; Nachtigall, H.; Pschorn, L.; Bauer, F.; Blind, K.; Martin, N.; Grafenstein, M. von; Streblow, R.; Du, J.; Schölzel, J. D. (2024): Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft : Bericht zu Arbeitspaket 1.2 : Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle ; Die Studie wird im Auftrag des Bundesministeriums für Bildung und Forschung (kofinanziert durch das Programm »NextGenerationEU» der Europäischen Union) durchgeführt. https://doi.org/10.18154/RWTH-2024-04375.

Kreutzer, S. et al. (2023): Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft. Bericht zu Arbeitspaket 1.2: Anforderungen und Umsetzungshemmnisse für Datentreuhandmodelle. Technopolis Group

Veil, W. (2021a): Data Governance Act II: Datenmittler. Online verfügbar unter https://www.cr-online.de/blog/2021/10/11/in-der-datenschutzrechtlichen-todeszone-der-data-governance-act-teil-ii/, zuletzt geprüft am 12.07.2024.

Veil, W. (2021b): Data Governance Act III: Datenaltruismus. Online verfügbar unter https://www.cr-online.de/blog/2021/10/28/data-governance-act-iii-datenaltruismus/, zuletzt geprüft am 12.07.2024.

Veil, W. (2021c): Data Governance Act IV: Dataismus. Online verfügbar unter https://www.cr-online.de/blog/2021/12/07/data-governance-act-iv-dataismus/, zuletzt geprüft am 12.07.2024.

Wagh und Mishra, 2023, »A distributed approach to privacy preservation and integrity

WindEurope (2023): Joint Industrial Statement on the Data Act. Online verfügbar unter https://windeurope.org/policy/joint-statements/joint-industrial-statement-on-the-data-act/, zuletzt geprüft am 12.07.2024.

Impressum

Herausgeber
Fraunhofer-Exzellenzcluster Integrierte Energiesysteme (CINES),
EUREF Campus 23 – 24, 10829 Berlin

Verantwortlich für den Inhalt des Textes
Volker Berkhout, volker.berkhout@iee.fraunhofer.de; Marian Klobasa, marian.klobasa@isi.fraunhofer.de; Nicholas Martin, nicholas.martin@isi.fraunhofer.de; Murat Karaboga, murat.karaboga@isi.fraunhofer.de; Jonathan Bergsträßer, jonathan.bergsträßer@iee.fraunhofer.de; Manuel Wickert, manuel.wickert@iee.fraunhofer.de; Junsong Du, junsong.du@eonerc.rwth-aachen.de; Rita Streblow, rstreb-low@eonerc.rwth-aachen.de; Lukas von der Heide, lukas.von.der.heide@iee.fraunhofer.de; Marijke Welisch, marijke.welisch@zv.fraunhofer.de

Beteiligte Institute
Fraunhofer Institut für Energiewirtschaft und Energiesystemtechnik IEE
Fraunhofer Institut für System und Innovationsforschung ISI
RWTH Aachen

Bildnachweis
Deckblatt: iStock/peshkov; S.6: iStock/imaginima; S.17: iStock/Laurence Dutton, S21: iStock/gorodenkoff

Zitierempfehlung
Berkhout, Volker; Klobasa, Marian; Martin, Nicholas; Karaboga, Murat; Bergsträßer, Jonathan; Wickert, Manuel; Du, Jungsong; Streblow, Rita; von der Heide, Lukas; Welisch, Marijke (2025): Implikationen der europäischen Datenstrategie und -regulierung für die Energiewirtschaft. Whitepaper. Karlsruhe, Kassel. Fraunhofer CINES.

Veröffentlicht
Februar 2025, Version 1.0

DOI
10.24406/publica-3988