Deutsche Stiftung für Recht und Informatik

Algorithmus trifft Recht: Informatik und EU Data Act im Wechselspiel?

Frank Sarre
Projective Expert Group, München & LMU München

12. September 2025 *Version v001*

Herbstakademie 2025

Einleitung

Data Act:	Einheitlicher Rechtsrahmen der EU für Datenzugang und -nutzung (VO (EU) 2023/2854)
Inhalt:	Klare Regeln, wer welche (insb. Industrie-) Daten unter welchen Bedingungen nutzen darf → Förderung datengesteuerter Innovation
Geltung:	Ab heute (12.09.2025)
Ziel:	Wettbewerbsfähiger, innovationsfreundlicher Datenbinnenmarkt; faire Verteilung des Datenwerts unter den Beteiligten
Pflicht für Hersteller vernetzter Produkte / Dienste:	„Access by Design“ → sicherer, einfacher Zugriff und Weiterverwendung durch Nutzer / autorisierte Dritte
Wechselwirkung Recht ↔ IT:	Rechtliche Bestimmungen prägen Architekturen, Schnittstellen, Zugänge, Funktionalitäten und Konfigurationen, Technik beeinflusst die Auslegung und wirft neue Rechtsfragen auf

- Hohe Praxisrelevanz für Unternehmen der digitalen Wirtschaft und IT-Compliance

Zielsetzung und Regulierungsansatz (1)

Ziele der Verordnung

- Faire Aufteilung des Datenwerts und breitere Nutzbarmachung für Wirtschaft / Gesellschaft / öffentliche Verwaltung
  → nachhaltiges Wachstum

- Zugriffs- und Weitergaberechte für Nutzer vernetzter Produkte
  → neue datengestützte Dienste & Wettbewerb
  → zusätzlich Rechtssicherheit
  → Investitionsanreize
  → breitere Teilhabe von Unternehmen aller Größen

Zielsetzung und Regulierungsansatz (2)

Regulatorischer Ansatz

- Gestaffelte Pflichten für betroffene Hersteller
- Sektorübergreifend und technologieoffen
- Setzt Prinzipien / Mindeststandards, lässt aber Raum für Selbstregulierung sowie industriegetriebene technische Ausgestaltung
- Verweis auf bestehende Normen der Standardisierungsorganisationen
- Weitere harmonisierte Standards zu erwarten
- Einrichtung eines zentralen Registers anerkannter technischer Spezifikationen

Zielsetzung und Regulierungsansatz (3)

Differenzierung nach Unternehmensgröße

- Kleinst-, Klein- und mittlere Unternehmen – inkl. Startups / Handwerkbetriebe – sind weitgehend von B2B-Datenbereitstellungspflichten ausgenommen („KMU-Privilegierung“);
  kein genereller Drittzugang zu Gerätedaten.

- B2G-Regelung:
  Gegenüber Behörden bleibt Auskunftspflicht bestehen
  (z.B. Gefahrenabwehr, Katastrophenfall)

- Größere Dateninhaber dürfen gegenüber kleinen Unternehmen nur Kostenersatz verlangen (keine Gewinnmargen!)
  → Entlastung und fairer Nutzen für KMUs

Zielsetzung und Regulierungsansatz (4)

Cloud-Portabilität und „Switching“

- Vermeidung eines Vendor-Lockins im Cloud-Bereich
- Portabilität & Interoperabilität verpflichtend,
  Abbau technischer und vertraglicher Wechselhürden
- Offene / standardisierte Formate & APIs
- Verbot überhöhter Data-Egress-Charges (über reine Extraktionskosten hinaus)
- Migration mit Schutzmaßnahmen:
  Verschlüsselung, Audits, angepasste Sicherheitsrichtlinien

Branchenreaktion (2024):

– Google Cloud & AWS streichen Egress-Gebühren

– Schaffung von mehr Migrationstools → nahezu nahtloserer Anbieterwechsel

Zielsetzung und Regulierungsansatz (5)

- **„Access by Design“**
  - Einfache und sichere Datenzugänglichkeit ist bereits bei Konzeption / Herstellung / Entwicklung vernetzter Produkte zu berücksichtigen;
    Umsetzungsspielraum
  - Geltung neben der DSGVO – „Privacy by Design“ bleibt unberührt!
    → Access by Design und Privacy by Design sind angemessen auszutarieren
  - Wahrung von Geschäftsgeheimnissen
  - Begrenzung der Informationsgewinnung
    - Zweckbindung
    - keine Wettbewerbsausforschung
    - kein sonstiger Missbrauch

Technische Umsetzungserfordernisse (1)

Datenzugangsarchitekturen, APIs

- Datenbereitstellung nahezu in Echtzeit + strukturiert + maschinenlesbar
  ⇒ leistungsfähige Datenzugangsarchitektur nötig
- APIs (RESTful/GraphQL) mit Filtern nach Zeitraum / Kategorien;
  für Dauerströme Streaming / WebSockets.
- Skalierbarkeit: Microservices, Cloud-native, API-Gateways, Caching,
  Load-Balancing (für die Handhabung von IoT-Lastspitzen)
- Zugriffskonzept: RBAC + IAM (OAuth 2.0 / OpenID Connect), MFA;
- Feingranulare Rechte / Least-Privilege für Dritte
  (z.B. nur Temperatur-/ Betriebsstunden, keine personenbezogenen Logs).
- Audit / Compliance: Revisionssicheres Logging sämtlicher Drittzugriffe
- Benutzerfreundlichkeit:
  Web-Dashboards / Mobile Apps als GUI für API-basierten Zugriff / Weitergabe

Technische Umsetzungserfordernisse (2)

Sicherheit und Verschlüsselung

- Schutz vs. offener Zugang: Privacy by Default bleibt Pflicht
- Schlüsselverwaltung / Delegation: Nutzer erhält Schlüssel;
  temporäre Freigaben für Dritte oder serverseitig entschlüsselte gesicherte APIs
- PETs: Tokenisierung / Pseudonymisierung mit Token-Vault beim Dateninhaber;
  Mapping nur bei Erforderlichkeit
  → Schutz von Personenbezug und Geschäftsgeheimnissen.
- Verschlüsselte Verarbeitung:
  (Teilweise) homomorphe Verschlüsselung für Analysen / ML beim Dienstleister;
  Rohdaten bleiben unlesbar – derzeit performancekritisch.
- Federated Learning: Modelle anstatt Daten zu teilen (z.B. AML, Mobile Keyboard);
  lokales Training, zentrale Aggregation;
  Datenschutz / Bankgeheimnis bleibt gewahrt.
- Zugriffsarchitektur härten: RBAC / IAM (OAuth2 / OIDC), MFA, feingranulare Rechte; revisionssicheres Logging aller Drittzugriffe
- Transportsicherheit & Cloud-Switching: TLS / Stand-der-Technik;
  Sicherheitsniveau beim Wechsel mindestens halten → Secure Access by Design

Technische Umsetzungserfordernisse (3)

Strukturierte Formate und Interoperabilität

- Bereitstellung von Daten: Einfach und unentgeltlich;
  offene, strukturierte, maschinenlesbare, interoperable Formate (keine proprietären)
- Standards: JSON / XML, CSV;
  Branchenstandards wie OPC UA (Industrie 4.0), FHIR/HL7 (Gesundheitswesen),
  IEC 61850 / DLMS-COSEM (Energiewirtschaft)
- Interoperabilität: Offene Spezifikationen, Referenz ISO/IEC 19941;
  syntaktisch und semantisch (gemeinsame Datenmodelle / Ontologien)
- Ökosysteme & Schnittstellen: Gaia-X / Catena-X als Enabler;
  SWIPO-Kodizes für Cloud-Wechsel / Export / Migration
- Praxis: Formate inventarisieren und auf Standards migrieren;
  Standard-APIs / Datenmodelle implementieren
  → weniger Lock-in, Data-Act-Konformität

Rechtliche Implikationen und Konfliktfelder (1)

Verhältnis zur DSGVO

- Die DSGVO gilt weiter:
  Personenbezogene Daten → DSGVO-Anwendung;
  Data Act hebt DSGVO nicht auf
  → Ausgleich zwischen „Access by Design“ und „Privacy by Design“ erforderlich.
- Rechtsgrundlage:
  Zulässigkeit der Herausgabe / Verarbeitung fallabhängig;
  praxisrelevant Einwilligung;
  heikel bei Drittpersonen in IoT-Daten (z.B. Mitfahrer).
- Restriktive Auslegung möglich:
  Zur Wahrung Zweckbindung / Datensparsamkeit können Data-Act-Zugriffsrechte eng interpretiert werden, wenn Drittdaten betroffen sind.
- Technische Ansätze: Federated Learning, Differential Privacy (Rauschen) zur Minimierung personenbezogener Bezüge ohne Rohdatenzentralisierung.
- Praxis: Einzelfallabwägung nach Datensensibilität;
  DSB/Legal einbinden;
  gerichtliche Praxis wird Leitplanken konkretisieren.

Rechtliche Implikationen und Konfliktfelder (2)

Schutz von Geschäftsgeheimnissen und vertraulichen Informationen

- Geschäftsgeheimnisse können gewahrt werden:
  Datenweitergabe unbeschadet des Geheimnisschutzes;
  keine Nutzung zur Ermittlung wirtschaftlicher Lage ohne Zustimmung.
- Vertragliche Absicherung:
  Definition geheimer Infos, Zweckbindung, Verschwiegenheit, sichere Aufbewahrung, Rückgabe / Löschung, keine Weitergabe an Dritte.
- Technische Minimierung: Selektion / Aggregation, Pseudonymisierung / Tokenisierung von IDs.
- Monitoring & Enforcement:
  Logging, Rate-Limiting, Anomalie-Alarme;
  bei Verstößen Zugang entziehen und Ansprüche durchsetzen.
- Praxisbeispiel: Smart-Geräte-Hersteller liefert nutzbare, aber nicht rückschlussfähige Daten an konkurrierenden Service.
- Vorgehen: Identifikation geheimer Inhalte, Erforderlichkeit prüfen, Schutzmaßnahmen (Entfernung / Abstraktion / NDA), Nutzungskontrolle.

Rechtliche Implikationen und Konfliktfelder (3)

Vertragliche Ausgestaltung und faire Nutzungsbedingungen

- AGB / EULAs / Datenklauseln auf Data-Act-Konformität prüfen;
  kategorische Weitergabeverbote streichen;
  Nutzerrechte, Drittzugriff und Support verankern.
- Entgelte nur kostenorientiert; pauschale / aufschlagende Fees entfernen.
- Fair, angemessen, nichtdiskriminierend („FRAND“);
  unfaire Klauseln – v.a. gegenüber KMUs – sind unwirksam.
- Musterklauseln kurz fassen:
  - Datenumfang / Granularität / Aktualität;
  - Zweckbindung / Löschung;
  - Weitergabeverbote;
  - Sicherheitsniveau;
  - Haftung;
  - Streitbeilegung / ADR
- Adressatengruppen trennen (B2C / B2B / B2G);
  Lock-in vermeiden (Laufzeit / Kündigung / Migration);
  Haftungsabgrenzung / Freistellung bei Drittweitergabe;
  flexibel & technologieneutral gestalten.

Handlungsempfehlungen und Compliance-Strategien (1)

Data-Governance-Frameworks

- Integrierte Data Governance:
  - Erstellung von Richtlinien zur Freigabe und Herausgabe von Daten
  - Definition von Verantwortlichkeiten
- „Data Release Board“ (Recht/IT-Security/Datenschutz/Fachbereiche):
  - Entscheidet über Zugriffe,
  - nimmt Standardisierungen vor
  - bewertet Risiken
- Lückenlose Dokumentation aller Datenweitergaben erforderlich
  (dabei sind Entscheidungsprotokolle zu führen, klare Rollen und Eskalationspfade)

Handlungsempfehlungen und Compliance-Strategien (2)

Interdisziplinäre Zusammenarbeit stärken

- Enge Zusammenarbeit von Recht, Datenschutz, IT-Security und Entwicklung nötig
- Data Act als Anlass, Organisations-„Silos“ aufzubrechen
- Gemeinsame Workshops / Schulungen:
  Legal erläutert Pflichten / Hintergründe / Vorteile;
  IT zeigt technische Möglichkeiten und Grenzen auf
- Abteilungsübergreifende Zusammenarbeit als Schlüssel zu praxisgerechten Lösungen
- Einrichtung eines Data Compliance Officers
  als Schnittstelle zwischen Technik und Recht in der Datenverwaltung
- Interdisziplinärer Ansatz beschleunigt die Compliance und hebt die Wertschöpfung; frühe Data-Act-Konformität schafft Vertrauen

Ausblick

Konkretisierungen / Standards:	Delegierte Rechtsakte & Durchführungsrechtsakte; CEN/CENELEC/ETSI für harmonisierte Normen; zentrales Standard-Repository; frühe Pilotteilnahme = Einfluss / Compliance-Vorsprung
Regelungsverbund:	Verzahnung mit AI Act (Datenqualität / Governance) – Synergien vs. KI-Beschränkungen
Globaler Referenzpunkt:	Außerhalb der EU kein Pendant zum Data Act; möglicher Blaupausen-Effekt (z.B. gestrichene Egress-Fees)
Paradigmen- & Kulturwandel:	Daten als geteilte Ressource; aktives Datenmanagement (rechtlich / technisch / organisatorisch)
Best Practices & Kompetenzen:	Interdisziplinär; Standard-APIs, Branchendatenmodelle, Vertragstemplates; Privacy & Security stets mitdenken!
Wettbewerbsfaktor & Zielbild:	Rechtssicheres Datenteilen wird Schlüsselkompetenz; Ergebnis: Vertrauenswürdiger, wettbewerbsfähiger EU-Datenmarkt Data Act als Kernstück der Digitalregulierung

Gerne Fragen !

Kontaktdaten

PD Dr. Frank Sarre

- Öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung
- Privatdozent an der LMU München, Fachbereich Informatik
- Handelsrichter am Landgericht München I

Projective Expert Group GmbH
Lindwurmstr. 149
80337 München

Telefon 089 / 18 92 37 -01
Mobil 0172 / 8 215 295
E-Mail: frank.sarre@projective.de