



AIGN Data Act AI Governance Framework

Patrick Upmann



The AIGN Data Act Governance Framework 1.0

Table of Content

0. MANAGEMENT SUMMARY.....	6
KEY OBJECTIVES	6
1.EXECUTIVE SUMMARY	7
WHY A NEW “OPERATING SYSTEM” FOR DATA & AI GOVERNANCE?	7
WHAT MAKES AIGN DIFFERENT?.....	8
KEY BENEFITS AND FEATURES	8
WHO IS THIS FRAMEWORK FOR?	8
THE AIGN ADVANTAGE:.....	9
2. EXECUTIVE ENTRY SECTION	10
EXECUTIVE POLICY BRIEFING: TURNING GOVERNANCE INTO STRATEGY	10
BUSINESS STRATEGY BRIEFING: TRUSTED DATA & AI AS A GROWTH DRIVER.....	11
3. WHY A NEW FRAMEWORK?	12
THE NEW REALITY: INTELLIGENT SYSTEMS, DATA-DRIVEN ECONOMIES, GLOBAL COMPLEXITY ..	12
USE CASES: WHY INTEGRATED DATA & AI GOVERNANCE IS NEEDED	13
GLOBAL PERSPECTIVE: EUROPE SETS THE PACE, THE WORLD RESPONDS	14
CONCLUSION: ONE FRAMEWORK, ONE JOURNEY.....	14
4. WHY AIGN?.....	16
AGN AS THE GLOBAL OPERATIONAL BACKBONE FOR DATA & AI GOVERNANCE.....	16
DATEN, FAKTEN, MARKTSTELLUNG	16
WHY EXISTING APPROACHES FALL SHORT	17
AGN'S UNIQUE VALUE PROPOSITION	17
5. WHAT IS THE AIGN EU DATA ACT AI GOVERNANCE FRAMEWORK?.....	18
A UNIFIED, OPERATIONAL SYSTEM FOR INTEGRATED DATA & AI COMPLIANCE	18
KEY FEATURES AND COMPONENTS	18
USE CASES: WHERE THE FRAMEWORK CREATES VALUE	20
GLOBAL PERSPECTIVE: BEYOND THE EU.....	21
LEGAL AND REGULATORY REFERENCES	21
CONCLUSION: THE OPERATIONAL COMPANION FOR THE NEXT DECADE.....	21
6. STRUCTURE & CORE PILLARS OF THE FRAMEWORK.....	22
STRUCTURED INTRODUCTION.....	22
FACTS & DATA.....	22
PILLARS TABLE/OVERVIEW	22
USE CASES & EXAMPLES.....	23
GLOBAL PERSPECTIVE.....	24
CONCLUSION & CALL TO ACTION.....	25



The AIGN Data Act Governance Framework 1.0

7. GOVERNANCE DOMAINS & LIFECYCLE	26
STRUCTURED INTRODUCTION.....	26
FACTS & DATA.....	27
CORE GOVERNANCE DOMAINS.....	27
LIFECYCLE PHASES & ACTIVITIES	27
USE CASES & EXAMPLES.....	28
GLOBAL PERSPECTIVE.....	30
8. DATA ACCESS & USER RIGHTS MANAGEMENT.....	30
MANAGEMENT SUMMARY	30
WHY DATA ACCESS & USER RIGHTS MANAGEMENT MATTER.....	30
KEY OBJECTIVES	30
9. MAPPING TABLE: REGULATORY REQUIREMENTS TO FRAMEWORK SOLUTIONS	31
MANAGEMENT SUMMARY	31
WHY A MAPPING TABLE?	31
TABLE STRUCTURE.....	31
MAPPING TABLE	31
IMPLEMENTATION NOTES	32
EXAMPLE USE	33
CORE IMPLEMENTATION REQUIREMENTS.....	33
USE CASE EXAMPLE	33
COMPLIANCE & CERTIFICATION CRITERIA.....	34
QUICK CHECKLIST FOR IMPLEMENTATION	34
CONTINUOUS IMPROVEMENT.....	34
10. RISK & IMPACT MAPPING.....	35
STRUCTURED INTRODUCTION.....	35
FACTS & DATA.....	35
RISK & IMPACT MAPPING DOMAINS	36
AIGN RISK TOOLS & METHODOLOGIES	36
USE CASES & EXAMPLES.....	37
GLOBAL PERSPECTIVE.....	38
11. COMPLIANCE & REGULATORY READINESS	39
STRUCTURED INTRODUCTION.....	39
FACTS & DATA.....	39
KEY COMPLIANCE DOMAINS & MAPPING.....	40
AIGN COMPLIANCE TOOLS & TEMPLATES	41
USE CASES & EXAMPLES.....	41
GLOBAL PERSPECTIVE.....	42
12. ASSESSMENT TOOLS & CERTIFICATION.....	43
STRUCTURED INTRODUCTION.....	43
FACTS & DATA.....	43



The AIGN Data Act Governance Framework 1.0

KEY ASSESSMENT TOOLS	44
CERTIFICATION LOGIC & MATURITY MODEL	44
USE CASES & EXAMPLES	45
GLOBAL PERSPECTIVE	46
13. ROLES, RESPONSIBILITIES & MATURITY MODEL	47
STRUCTURED INTRODUCTION	47
FACTS & DATA	47
RACI MODEL FOR DATA & AI GOVERNANCE	47
RACI IN PRACTICE:	48
MATURITY MODEL	48
USE CASES & EXAMPLES	49
GLOBAL PERSPECTIVE	50
CONCLUSION & CALL TO ACTION	50
14. PRACTICAL APPLICATION & USE CASES	51
STRUCTURED INTRODUCTION	51
KEY USE CASES	51
ADDITIONAL APPLICATION SCENARIOS	53
GLOBAL PERSPECTIVE	53
CONCLUSION & CALL TO ACTION	53
15. INTEGRATION WITH INTERNATIONAL STANDARDS	54
STRUCTURED INTRODUCTION	54
FACTS & DATA	54
KEY STANDARDS & REGULATORY MAPPING	55
BRIDGING GLOBAL GAPS:	55
USE CASES & EXAMPLES	56
GLOBAL PERSPECTIVE	57
CONCLUSION & CALL TO ACTION	57
16. DATA & AI LITERACY – EMPOWERING COMPLIANCE, TRUST, AND INNOVATION	58
STRUCTURED INTRODUCTION	58
FACTS & DATA	58
KEY COMPONENTS & TOOLS	58
REGULATORY LINK	59
USE CASES	59
GLOBAL PERSPECTIVE	59
17. DATA ALTRUISM & RESPONSIBLE DATA SHARING	59
STRUCTURED INTRODUCTION	59
FACTS & DATA	59
CORE ELEMENTS & TOOLS	60
REGULATORY LINK	60
USE CASES	60



The AIGN Data Act Governance Framework 1.0

GLOBAL PERSPECTIVE.....	60
CONCLUSION & CALL TO ACTION	61
18. PEER LEARNING, INCIDENT SHARING & CONTINUOUS IMPROVEMENT	61
STRUCTURED INTRODUCTION	61
FACTS & DATA.....	61
CORE ELEMENTS & TOOLS	61
REGULATORY LINK	61
USE CASES	61
GLOBAL PERSPECTIVE.....	62
CONCLUSION & CALL TO ACTION	62
19. TECHNICAL REFERENCE ARCHITECTURES & INTEGRATION BLUEPRINTS	62
FACTS & DATA.....	62
CORE ELEMENTS & TOOLS	62
REGULATORY LINK	63
USE CASES	63
GLOBAL PERSPECTIVE.....	63
20. TRUSTED DATA INTERMEDIARIES & DATA TRUSTEE MODELS (DGA INTEGRATION)	63
FACTS & DATA:.....	64
KEY FEATURES & DELIVERABLES:	64
USE CASES:	64
GLOBAL PERSPECTIVE:.....	64
CONCLUSION & CALL TO ACTION:	64
21. DATA ALTRUISM & RESPONSIBLE DATA SHARING (DGA INTEGRATION)	65
FACTS & DATA:.....	65
KEY FEATURES & DELIVERABLES:	65
USE CASES:	65
GLOBAL PERSPECTIVE:.....	65
22. REGISTRATION, OVERSIGHT & CERTIFICATION OF DATA INTERMEDIARIES (DGA INTEGRATION)	66
FACTS & DATA:.....	66
KEY FEATURES & DELIVERABLES:	66
USE CASES:	66
23. TECHNICAL AND ORGANIZATIONAL REQUIREMENTS FOR SECURE DATA ENVIRONMENTS (DGA/DA INTEGRATION)	67
FACTS & DATA:.....	67
KEY FEATURES & DELIVERABLES:	67
USE CASES:	68
GLOBAL PERSPECTIVE:.....	68
24. STAKEHOLDER ENGAGEMENT, TRANSPARENCY & DISPUTE RESOLUTION (DGA/DA INTEGRATION)	68



The AIGN Data Act Governance Framework 1.0

FACTS & DATA:	68
KEY FEATURES & DELIVERABLES:	68
USE CASES:	69
GLOBAL PERSPECTIVE:	69
CONCLUSION & CALL TO ACTION:	69
SUMMARY FOR IMPLEMENTATION	69
25. CONTRACTUAL FAIRNESS & STANDARD CLAUSES MODULE	69
MANAGEMENT SUMMARY	69
WHY CONTRACTUAL FAIRNESS MATTERS	69
KEY OBJECTIVES	70
CORE IMPLEMENTATION REQUIREMENTS	70
USE CASE EXAMPLE	71
COMPLIANCE & CERTIFICATION CRITERIA	71
QUICK CHECKLIST FOR IMPLEMENTATION	71
CONTINUOUS IMPROVEMENT	71
26. FRAMEWORK GOVERNANCE, USAGE AND LICENSING	71
LEGAL STRUCTURE AND INTELLECTUAL OWNERSHIP	72
PERMITTED USES (OPEN ACCESS – NON-COMMERCIAL)	74
PERMITTED:	74
NOT PERMITTED WITHOUT PRIOR WRITTEN AGREEMENT:	75
PROTECTED ELEMENTS (USE REQUIRES LICENSE OR PARTNERSHIP)	75
COMMERCIAL USE & DERIVATIVE WORKS	75
ATTRIBUTION REQUIREMENTS	76
CERTIFIED PARTNERSHIP AND LICENSING	76
ENFORCEMENT AND JURISDICTION	77
CLOSING STATEMENT	77
27. APPENDIX: GLOSSARY & DEFINITIONS	78
MANAGEMENT SUMMARY	78
KEY TERMS & DEFINITIONS	78



The AIGN Data Act Governance Framework 1.0

AIGN Data Act AI Governance Framework 1.0

Operationalizing Trust for Autonomous, Self-Improving, and Multi-Agent AI Systems
Version 1.0 | © 2025 AIGN – Artificial Intelligence Governance Network

0. Management Summary

The convergence of data and artificial intelligence (AI) is transforming every sector—accelerating innovation, value creation, and societal progress. Yet, with this opportunity comes unprecedented regulatory, ethical, and operational challenges. The entry into force of the **EU Data Act (from September 2025)**, together with the **EU AI Act** and **GDPR**, creates a new era of accountability:

Organizations must not only use data and AI responsibly, but also **prove** compliance, fairness, and trust—across the entire data and AI lifecycle.

The **AIGN EU Data Act AI Governance Framework** provides a unified, actionable structure for integrating data and AI governance—bridging legal requirements, technical standards, and operational best practices. It enables organizations of all sizes to build trust, unlock innovation, and demonstrate compliance in a dynamic regulatory landscape.

Key Objectives

- **Full compliance** with EU Data Act, EU AI Act, GDPR, Data Governance Act, NIS2, and other leading standards.
- **Integrated Data & AI Governance:** One framework, one lifecycle, from data collection to AI deployment and ongoing monitoring.
- **Actionable tools & certification:** Maturity assessments, readiness scans, practical checklists, and trust labels.
- **Scalable & modular:** For startups, SMEs, large enterprises, public sector, and global deployments.
- **Trust as competitive advantage:** Turning compliance from a cost into a growth driver.



The AIGN Data Act Governance Framework 1.0

Each key objective directly addresses major requirements of the EU Data Act, AI Act, and other leading regulations—ensuring organizations reduce compliance risk while enabling business growth through trustworthy data and AI practices.

Global Benchmark

Unlike most existing governance frameworks, AIGN operationalizes and fully aligns with ISO/IEC 42001, OECD AI Principles, and NIST AI RMF, but goes further by providing actionable tools, continuous certification, and up-to-date regulatory mapping.

Key Takeaway:

The AIGN Framework transforms regulatory complexity into an operational and certifiable approach, enabling both EU-based and international organizations to turn compliance into a driver for trust, market access, and innovation.

1.Executive Summary

AIGN EU Data Act AI Governance Framework

The Operating System for Responsible Data & AI in a Regulated World

The world has entered the age of intelligent, connected systems—where data and AI are no longer just enablers, but the foundation of value, competition, and societal progress. In this new era, regulatory complexity and public expectations have reached unprecedented levels: the EU Data Act, EU AI Act, and Data Governance Act (DGA) collectively redefine what it means to use data and AI responsibly, lawfully, and competitively.

Why a New “Operating System” for Data & AI Governance?

- **Regulatory Tsunami:** From September 2025, organizations across Europe (and any entity serving EU users) face a new, integrated compliance reality. The EU Data Act mandates fair, secure, and interoperable data access. The EU AI Act introduces risk-based governance, transparency, and human oversight for all AI systems. The DGA establishes new standards for data intermediaries, data altruism, and cross-border data ecosystems.
- **Global Convergence:** The “Brussels Effect” ensures that these standards rapidly become the blueprint for global markets—mirrored in ISO/IEC 42001, OECD AI Principles, NIST AI RMF, and adopted by regulators worldwide.



The AIGN Data Act Governance Framework 1.0

What Makes AIGN Different?

The AIGN Framework is not just another compliance checklist.

It is a fully integrated, certifiable “Operating System” for Data & AI Governance—translating every article, obligation, and best practice from the EU Data Act, AI Act, and DGA into actionable, measurable, and auditable practice.

It unifies legal, technical, and organizational requirements into a single, modular architecture—covering the entire lifecycle, from data generation and sharing, to AI model development, deployment, and ongoing monitoring.

Key Benefits and Features

- **Total Regulatory Coverage:** Every chapter, template, and tool is mapped to the key obligations of the EU Data Act (data access, portability, fairness), EU AI Act (risk, transparency, quality), and DGA (trusted intermediaries, data altruism, stakeholder engagement).
- **Operational Excellence:** Includes practical toolkits, audit templates, contract modules, readiness assessments, trust labels, and certification logic.
- **Continuous Compliance:** Embeds maturity models, incident sharing, peer learning, and continuous improvement cycles—ensuring organizations are always audit-ready and future-proof.
- **International Adaptability:** Harmonized with global standards; supports multinational, SME, public sector, and cross-border collaboration.
- **Trust & Innovation:** Turns compliance into a driver for growth, market access, and digital trust—building confidence with regulators, partners, investors, and society.

Who Is This Framework For?

- **Enterprises & SMEs:** Transform compliance from a burden into a competitive advantage; unlock new markets with proof of trust.
- **Public Sector & Regulators:** Ensure digital sovereignty, public accountability, and harmonized implementation of EU law.
- **Startups & Innovators:** Rapid, modular onboarding for high-growth teams—no legal department required.
- **Consultancies & Partners:** Deliver turnkey compliance, certification, and audit solutions at scale.
- **International Organizations:** Achieve seamless alignment with the strictest global requirements.



The AIGN Data Act Governance Framework 1.0

The AIGN Advantage:

- **Actionable, scalable, certifiable.**
- **The only system where every regulatory obligation becomes a practical tool, workflow, or template—making compliance, trust, and innovation measurable and operational.**

AIGN is the backbone of the new digital economy.

It is the reference Operating System for every organization that wants to lead, not just follow, in the age of responsible, regulated data and AI.

The framework provides direct operational mapping to ISO/IEC 42001, OECD AI Principles, NIST AI RMF, UNESCO AI Ethics, and more.

For more, see www.aign.global or contact your AIGN Partner for onboarding and licensing.

AIGN Core Pillars vs. International Standards – Quick Reference Table

Quick Reference Table: How AIGN Pillars Map to EU & Global Standards

AIGN Pillar	EU Data Act	EU AI Act	DGA	OECD AI Principles	ISO/IEC 42001	NIST AI RMF	UNESCO AI Ethics
1. Trust & Capability Indicators	Data access, fairness (Art. 3–13), transparency	Transparency, explainability (Art. 13–16)	Trust, stakeholder engagement, data altruism (Ch. III, V)	Fairness, transparency, accountability	Transparency, explainability, roles	Explainability, trustworthy AI	Human rights, inclusiveness, transparency
2. Governance Maturity & Lifecycle	Documentation, audit, lifecycle (Art. 4, 23–24)	Risk management, post-market monitoring (Art. 9, 19)	Registration, oversight (Art. 16–17)	Accountability, risk management, robustness	Governance structure, continuous improvement	Governance, monitoring, continuous learning	Multi-stakeholder, lifecycle perspective



The AIGN Data Act Governance Framework 1.0

AIGN Pillar	EU Data Act	EU AI Act	DGA	OECD AI Principles	ISO/IEC 42001	NIST AI RMF	UNESCO AI Ethics
3. Risk & Impact Mapping	Risk mapping, data misuse, security (Art. 24, 33)	Risk management, high-risk AI (Art. 8–19)	Intermediary breach prevention	Robustness, safety, risk management	Risk assessment, mitigation	Risk identification, assessment, mitigation	Societal & ethical risk, impact
4. Compliance Readiness & Certification	Contractual fairness, interoperability, audit (Art. 13, 23–24)	Technical documentation, auditability (Art. 18–19)	Certification, transparency, reporting	Certification, standards alignment	Certification, audit, maturity	Assessment, documentation, certification	Ethics, transparency, audit
5. Data Access & User Rights Management	User access, export, rights (Art. 4, 13, 23)	User rights, human oversight (Art. 16, 22)	Consent, data subject rights	Human-centric values, user empowerment	Data subject rights, user controls	User-centric design, transparency	Human dignity, consent, rights
6. Stakeholder Engagement & Peer Learning	Dispute resolution, transparency (Art. 18)	Stakeholder feedback, human oversight	Engagement, transparency (Art. 8, 18)	Inclusive growth, stakeholder participation	Stakeholder input, transparency	Stakeholder engagement	Public participation, inclusive governance
7. Technical Reference Architectures	API, data portability, technical interoperability (Art. 23–24)	Technical documentation (Art. 17, 19)	Secure processing environments	Interoperability, standards	Technical controls, architecture	Technical robustness	Technology for good, openness

2. Executive Entry Section

Executive Policy Briefing: Turning Governance into Strategy



The AIGN Data Act Governance Framework 1.0

For policymakers, regulators, and public sector leaders

Purpose:

To provide a strategic roadmap for aligning national and institutional practices with the EU Data Act & AI Act, ensuring legal certainty, public trust, and digital sovereignty. International governments and agencies can adopt AIGN modules to rapidly harmonize national requirements with EU law, ISO, and local frameworks—accelerating regulatory convergence and market entry.

Key Highlights:

Domain	Framework Value
Data & AI Regulation	Translates EU Data Act & AI Act into practical, operational policies
Public Accountability	Enables transparency, auditability, and redlining for data & AI
Interoperability	Supports harmonization with GDPR, DGA, NIS2, OECD, UNESCO, and NIST
Strategic Control	Empowers ministries to standardize or recommend data/AI governance
Certification	Offers readiness checks and trust labels for public and private sector

Actions for Ministries & Agencies:

- Integrate Trust & Readiness Scans into AI/data-intensive public projects
- Use the AIGN Trust Label for procurement, funding, and digital policy alignment
- Leverage modular tools for audit, reporting, and policy impact assessment

Business Strategy Briefing: Trusted Data & AI as a Growth Driver

For CEOs, boards, innovation, data & compliance leaders

Purpose:

To empower organizations to transform regulatory pressure into an opportunity for innovation, efficiency, and stakeholder trust.

Key Highlights:



The AIGN Data Act Governance Framework 1.0

Driver	Framework Contribution
Market Access	Meets EU and global regulatory requirements for data and AI
Customer Trust	Provides evidence of responsible data and AI use (trust labels, audit trails)
Innovation	Unlocks value through compliant, shareable, high-quality data
Risk Management	Reduces liability by operationalizing data rights, transparency, and fairness
Scaling Readiness	Offers modular, low-barrier entry and pathways to full certification

Actions for Enterprises & Startups:

- Use the Readiness Check to benchmark compliance and build investor confidence
- Apply modular policies and templates for rapid, cost-effective rollout
- Leverage sector-specific checklists for finance, health, mobility, public sector, etc.
- Certify compliance and maturity to unlock new markets and partnerships

3. Why a New Framework?

The New Reality: Intelligent Systems, Data-Driven Economies, Global Complexity

The world is entering an era where **data and AI are no longer just enablers—but core drivers of value, competition, and societal change**. By 2026, **over 80% of European businesses** expect the **EU Data Act** and **EU AI Act** to fundamentally impact their operations (IDC Europe, 2024). Globally, the volume of data is projected to reach **181 zettabytes by**



The AIGN Data Act Governance Framework 1.0

2025 (Statista, 2024), with more than **90% of all AI models** now relying on data that is not generated or owned by the organization itself.

Key Market and Regulatory Facts

- **Data is the foundation of AI:** No trustworthy AI system can exist without robust, transparent, and lawful data governance.
- **Connected devices (IoT):** In 2024, there are more than **17 billion IoT devices** worldwide—each producing valuable, often sensitive data (IoT Analytics, 2024). The **EU Data Act** specifically targets these devices, demanding that all data generated be accessible, portable, and reusable for users and authorized third parties (EU Data Act, Art. 3-4).
- **AI Regulation is here:** The **EU AI Act** introduces strict obligations for high-risk AI systems, including requirements for data quality, risk management, human oversight, and post-market monitoring (EU AI Act, Ch. 2-3).
- **Cross-border, cloud-first world:** Legacy compliance models—designed for closed, local data silos—are insufficient for today's **borderless, cloud-native, AI-powered value chains**.

Fragmentation and Silos: The Compliance Gap

- **Patchwork regulation:** Organizations are confronted with a **growing jungle of laws**—from GDPR (privacy), Data Governance Act (data altruism and trust), EU Data Act (data access, portability, interoperability), to sectoral and national requirements.
- **Siloed governance:** Most companies manage data, AI, and IT risks in **separate silos**, with disconnected teams, policies, and reporting. This leads to gaps, inefficiencies, and increased risk of compliance failures.

Legal, Ethical, and Technical Complexity

- **Traceability & explainability:** The **EU Data Act** requires all organizations to **document and provide access to the origin, format, and quality of data** (Art. 3, 4, 23)—a prerequisite for both trust and legal certainty.
- **Accountability:** The **AI Act** demands that high-risk AI systems are not just technically robust, but also auditable and explainable—**organizations must prove, not just promise, compliance** (EU AI Act, Art. 16-17).
- **Ethical challenges:** Discrimination, bias, and exclusion are not theoretical risks. Studies show that AI systems trained on poor or non-representative data often perpetuate or amplify societal harms (Stanford AI Index, 2024). The Data Governance Act encourages responsible data sharing and data altruism, but without operational governance, the risk of unintended harm grows.

Use Cases: Why Integrated Data & AI Governance is Needed



The AIGN Data Act Governance Framework 1.0

1. Connected Mobility & Smart Devices (IoT)

Case: An automotive supplier in Germany collects real-time data from smart vehicles across the EU.

Challenge: Under the **EU Data Act**, the company must allow drivers, fleet operators, or authorized third parties access to all relevant in-vehicle data—while simultaneously protecting privacy (GDPR), trade secrets, and security (Data Act, Art. 4, 6, 7).

AI Link: If the data is used to train predictive maintenance AI models, both the data lineage (Data Act) and model explainability (AI Act) must be documented and auditable.

2. Healthcare AI

Case: A hospital uses an AI system to analyze patient data and support diagnostics.

Challenge: The system must comply with **GDPR** (for health data), **EU Data Act** (for device-generated data, e.g., wearables), and the **AI Act** (if classified as high-risk).

Consequence: Failure to implement unified governance can result in regulatory fines, patient distrust, and loss of data-sharing privileges.

3. B2B Platforms & Data Ecosystems

Case: A cloud platform enables manufacturers and service providers to exchange machine data and analytics.

Challenge: The platform must ensure **contractual fairness** (Data Act, Art. 13), interoperability (Data Act, Art. 23-24), and non-discriminatory access—across multiple jurisdictions.

AI Link: If analytics involve AI, the platform must also track **data provenance** and AI model risk classification.

Global Perspective: Europe Sets the Pace, the World Responds

- **EU as global rulemaker:** The **Brussels Effect** is real—non-European companies must adapt to EU standards if they wish to access the world’s largest digital market.
- **OECD AI Principles, ISO/IEC 42001, and NIST AI RMF:** All converge on the need for integrated, operational governance that bridges data, AI, and ethics.
- **Emerging markets:** For Africa, Asia, and Latin America, harmonized frameworks (like AIGN) are essential to ensure that global companies and local innovators can compete and cooperate on equal, trusted terms.

Conclusion: One Framework, One Journey



The AIGN Data Act Governance Framework 1.0

The era of isolated compliance is over.

Organizations must adopt a **single, integrated governance system** that covers the entire data and AI lifecycle—making compliance, trust, and innovation measurable, auditable, and scalable.

The **AIGN EU Data Act AI Governance Framework** is that harmonized, operational answer—turning complex legal obligations into practical, competitive advantage.

„Barriers to data sharing prevent optimal distribution of data for the benefit of society... A harmonised framework must be created that specifies who is entitled to use product data or related service data, under what conditions and on what basis“

Comparison with Traditional Approaches:

Unlike traditional compliance frameworks that focus on isolated legal obligations, the AIGN Framework delivers an integrated, operational system—bridging legal, technical, and ethical requirements while accelerating global market access.

Global Adoption Challenge:

Non-EU organizations face additional hurdles in aligning with EU data and AI laws. The AIGN Framework addresses this by offering tailored onboarding guidance and tools for cross-border compliance.

Pain Point vs. Regulation Table

Pain Point vs. Regulation Table

The following table maps core compliance challenges to the relevant EU regulations addressed by the AIGN Framework.

Pain Point / Challenge	EU Data Act	EU AI Act	Data Governance Act (DGA)	How AIGN Framework Addresses This
Siloed data & AI governance	✓	✓	✓	Integrated lifecycle management
Lack of data access/portability	✓ (Art. 3–8, 23)		✓	Standardized access/portability tools
Insufficient user rights/consent handling	✓ (Art. 4, 13)	✓ (Art. 16, 22)	✓	User rights dashboards, consent templates
Fragmented risk management	✓ (Art. 23–24)	✓ (Art. 9, 29)	~	Unified risk & impact mapping



The AIGN Data Act Governance Framework 1.0

Pain Point / Challenge	EU Data Act	EU AI Act	Data Governance Act (DGA)	How AIGN Framework Addresses This
Opaque AI decisions/bias		✓ (Art. 10, 13)	~	Model cards, explainability modules
Contractual unfairness	✓ (Art. 13, 23)		~	Standard clause templates, review checklists
No trusted intermediary/neutral party			✓ (Ch. III)	Data intermediary & trustee modules
Lack of auditability/documentation	✓	✓	✓	Audit trails, documentation, certification
Poor stakeholder engagement/complaints	~	~	✓ (Art. 18)	Transparency, dispute resolution toolkits

“To further clarify regulatory alignment, the following table highlights which pain points are directly addressed by each EU regulation and by which modules of the AIGN Framework.”

4. Why AIGN?

AIGN as the Global Operational Backbone for Data & AI Governance

In a world of converging data, AI, and rapidly evolving regulation, **AIGN (Artificial Intelligence Governance Network)** provides what most organizations lack: a **practical, modular, and globally aligned governance system** that translates complex legal requirements into measurable, certifiable practice.

Daten, Fakten, Marktstellung



The AIGN Data Act Governance Framework 1.0

- **Global adoption & recognition:**
AIGN supports organizations across 30+ countries—including EU member states, the Global South, the US, and Asia—helping them align with the EU Data Act, EU AI Act, Data Governance Act, and international standards (OECD AI Principles, ISO/IEC 42001, NIST AI RMF).
- **Community impact:**
Over **1,500+ members**, including ministries, SMEs, large corporates, and academic leaders, rely on AIGN for practical tools, assessment, and certification.
- **Continuous evolution:**
The framework is updated in real time to reflect new laws, regulatory guidance, and best practice—something static compliance manuals cannot offer.

Why Existing Approaches Fall Short

- **Siloed compliance is obsolete:**
Most organizations separate data governance (focused on GDPR/privacy) and AI governance (focused on ethics or risk)—leading to **gaps**, duplicated efforts, and audit fatigue.
- **Law ≠ Implementation:**
Regulations like the **EU Data Act** and **AI Act** are complex, with overlapping, sometimes ambiguous requirements. Practical translation into daily operations, contracts, technical design, and ongoing monitoring is lacking.
- **Lack of operational tools:**
Many frameworks (OECD, ISO, etc.) set high-level principles, but fail to provide **ready-to-use templates, assessment tools, and certification logic**.

AIGN's Unique Value Proposition

AIGN bridges this gap with:

- **Integrated Data & AI Lifecycle Governance:**
One framework, one audit, one proof—covering every step from data generation (Data Act: Art. 3-5), contractual design (Art. 13), interoperability (Art. 23), through AI model training (AI Act: Art. 10), risk classification, deployment, and incident response.
- **Actionable, modular toolkits:**
Self-assessments, readiness checks, contract templates, risk registers, data provenance logs, incident response plans—all mapped to Data Act and AI Act requirements.
- **Trust Labels & Certification:**
Demonstrate compliance and maturity, not just to regulators, but also to business partners, investors, and customers—essential for cross-border deals and public sector contracts.



The AIGN Data Act Governance Framework 1.0

- **Global standard, locally adaptable:**
Tools, guidance, and community learning enable organizations in Africa, Asia, the Americas and Europe to meet global standards while honoring regional laws, languages, and priorities.

Feature	AIGN	ISO/IEC 42001	NIST AI RMF	OECD Principles
Regulatory Mapping	Full	Partial	Partial	Principles
Actionable Tools	Yes	Limited	No	No
Certification Program	Yes	Yes	No	No
Update Cycle	Continuous	Infrequent	Ad hoc	Infrequent
Local Adaptation	Yes	Moderate	Moderate	Moderate

„To meet the needs of the digital economy and remove the obstacles to a smoothly functioning internal market for data, a harmonised framework must be created“

5. What Is the AIGN EU Data Act AI Governance Framework?

A Unified, Operational System for Integrated Data & AI Compliance

The **AIGN EU Data Act AI Governance Framework** is a modular, scalable, and certifiable structure designed to translate the complex requirements of the EU Data Act, EU AI Act, GDPR, and Data Governance Act into practical action.

It enables organizations to manage **the entire data and AI lifecycle**—from raw data access and sharing to the development, deployment, and monitoring of AI—through a single, unified governance system.

Key Features and Components

a) Four Core Pillars

1. Trust & Capability Indicators

- **What it covers:** Transparency, fairness, security, privacy, explainability, interoperability, and accountability.



The AIGN Data Act Governance Framework 1.0

- **Value** : Provides measurable benchmarks to communicate and assess governance maturity both internally and externally.
- 2. **Governance Maturity & Lifecycle Management**
 - **What it covers** : Roles and responsibilities (RACI), documentation, escalation protocols, handover points, auditability, and continuous improvement logic.
 - **Value** : Ensures that every step—from data generation (EU Data Act Art. 3-4) to AI model deployment (EU AI Act Ch. 2-3)—is governed, documented, and traceable.
- 3. **Risk & Impact Mapping**
 - **What it covers** : Legal, ethical, technical, and societal risks (e.g., data misuse, bias, exclusion, security breaches, contractual disputes).
 - **Value** : Provides heatmaps, risk registers, and templates aligned to both Data Act and AI Act requirements (e.g., risk classification, incident response).
- 4. **Compliance Readiness & Certification**
 - **What it covers** : Checklists, templates, readiness scans, and self-assessments mapped to each regulatory obligation (Data Act, AI Act, GDPR, DGA, NIS2, sectoral standards).
 - **Value** : Enables audit-proof compliance, readiness for regulatory review, and market-facing trust labels.

Quick Reference:

The four pillars—Trust & Capability Indicators, Governance Maturity, Risk & Impact Mapping, Compliance Readiness—each deliver practical tools, such as self-assessments, risk templates, and certification logic.

Direct Benefit:

For each pillar, users receive actionable templates and checklists that can be immediately implemented, supporting faster compliance and audit readiness.

Cross-border Acceptance:

The framework’s alignment with global standards accelerates procurement, contract negotiation, and regulatory approval for organizations entering the EU or partnering with European clients.

b) One Lifecycle, Full Integration

The framework maps every stage of the data-AI continuum:

- **Data generation & collection:**
Ensuring lawful, fair, and transparent collection from devices, users, or third-party sources (Data Act Art. 3, 4; GDPR Art. 5).



The AIGN Data Act Governance Framework 1.0

- **Data access & sharing:**
Enforcing fair, non-discriminatory, and auditable access and contractual logic (Data Act Art. 4-7, 13).
- **Data quality & provenance:**
Documenting data lineage, metadata, and ensuring data portability and interoperability (Data Act Art. 23-24; DGA).
- **AI model development & training:**
Quality and lawfulness of training data, risk classification, and bias checks (AI Act Art. 10-13).
- **AI deployment & monitoring:**
Ongoing risk and compliance monitoring, human oversight, and incident response (AI Act Art. 16-19).
- **Lifecycle review & improvement:**
Regular audits, feedback loops, recertification, and continuous improvement.

c) Practical Tools and Deliverables

- **AIGN Data & AI Readiness Check:** Self- and external assessments for Data Act/AI Act maturity.
- **Trust Label & Certification:** Market- and regulator-facing proof of compliance, transparency, and responsible practice.
- **Templates & Toolkits:** Contracts, data sharing agreements, RACI charts, model cards, privacy statements, incident playbooks.
- **Heatmaps & Risk Registers:** Customizable, real-time tools for identifying and mitigating risk at every stage.
- **Maturity Model:** Five levels, from Initial (ad hoc) to By Design (fully embedded, continuous improvement).

Use Cases: Where the Framework Creates Value

1. IoT & Smart Device Ecosystems

A smart home manufacturer uses the framework to:

- Enable secure, user-centric access to device data (Data Act Art. 3, 4).
- Document data provenance and quality for downstream AI analytics.
- Provide customers with certified trust labels to boost market confidence.

2. Health & Life Sciences

A cross-border health platform applies the framework to:

- Fulfill Data Act and GDPR requirements for patient-generated data.



The AIGN Data Act Governance Framework 1.0

- Track and document data used in high-risk AI diagnostic tools (AI Act).
- Certify ethical and legal compliance for insurance partners and regulators.

3. B2B Data Platforms

A cloud-based industrial platform leverages the framework to:

- Operationalize non-discriminatory data sharing (Data Act Art. 13, 23).
- Audit AI-powered analytics for bias, transparency, and security.
- Deliver compliance and trust labels that unlock new B2B partnerships.

Global Perspective: Beyond the EU

- **The “Brussels Effect”:**
The EU’s regulatory models for data and AI set the standard for global operations; the framework allows organizations worldwide to anticipate and align with EU law—de-risking market entry, partnerships, and procurement.
- **OECD, ISO/IEC, NIST, DGA Alignment:**
The framework’s structure is mapped to the world’s leading data and AI governance standards and can be localized for any region or sector.
- **Enabling Digital Sovereignty:**
Countries and organizations outside the EU use AIGN to build their own trusted, interoperable, and internationally recognized compliance programs.

Legal and Regulatory References

- **EU Data Act (Regulation (EU) 2023/2854):**
Sets horizontal rules for fair access, use, and sharing of data across B2C, B2B, and B2G settings—making user rights, data portability, and contractual fairness central obligations [【22:eu-data-act-deutsche-fassung-22-12-23.pdf】](#) [【21:vbw-Leitfaden-Data-Act-September-2024-2.pdf】](#) .
- **EU AI Act:**
Introduces a risk-based system, transparency, and human oversight requirements for AI systems, with explicit cross-references to the lawfulness, quality, and documentation of input data.
- **EU Data Governance Act (DGA):**
Establishes trusted data intermediaries, data altruism, and standards for responsible data sharing.
- **GDPR:**
Remains the “gold standard” for personal data protection—fully integrated within the AIGN framework’s logic.

Conclusion: The Operational Companion for the Next Decade



The AIGN Data Act Governance Framework 1.0

The AIGN EU Data Act AI Governance Framework is more than a compliance tool—it is the **operational backbone** for responsible, innovative, and globally competitive organizations.

It is **not another checklist**, but a living, certifiable system that enables:

- Measurable trust
- End-to-end accountability
- Continuous adaptation to law, technology, and market needs

6. Structure & Core Pillars of the Framework

Structured Introduction

The AIGN EU Data Act AI Governance Framework is intentionally designed as a **holistic, modular architecture**. This ensures that organizations can navigate the full spectrum of obligations and risks created by the convergence of data, AI, and digital business models—across sectors and jurisdictions.

Unlike traditional, siloed approaches, AIGN’s framework connects the **entire lifecycle**: from data collection, access, and sharing, through to AI model development, deployment, and continuous oversight.

Facts & Data

- **Regulatory Coverage:** The EU Data Act (Reg. 2023/2854) comes into force in September 2025, requiring organizations to implement horizontal, cross-sectoral data governance covering access, portability, contract fairness, and interoperability [22:eu-data-act-deutsche-fassung-22-12-23.pdf] .
- **AI Integration:** Over **85% of organizations** plan to deploy AI that will process or depend on third-party and IoT-generated data (McKinsey, 2024). This data must now be governed, documented, and explainable—per both the Data Act and EU AI Act.
- **Complex Ecosystems:** More than **60% of compliance failures** in AI-driven businesses are due to fragmented or missing data lineage, inconsistent contract terms, or lack of interoperability (Gartner, 2024).

Pillars Table/Overview



The AIGN Data Act Governance Framework 1.0

Pillar	Key Features & Deliverables	Regulatory Link
Integrated Data & AI Lifecycle Governance	End-to-end controls from data creation to AI deployment; unifies data, AI, and contract governance.	Data Act Art. 3-5, 13; AI Act Ch. 2-3
Trust & Capability Indicators	Metrics for transparency, fairness, privacy, security, explainability, interoperability, and accountability.	Data Act Art. 23-24; AI Act Art. 10, 13, 16
Governance Maturity & Lifecycle Management	RACI model, escalation paths, documentation, auditability, continuous improvement, regular reviews.	Data Act Art. 3, 4, 23; AI Act Art. 17, 19
Risk & Impact Mapping	Heatmaps, risk registers, and templates for legal, ethical, technical, and societal risk assessment and response.	Data Act Art. 23; AI Act Art. 9, 29; DGA Ch. 3
Compliance Readiness & Certification	Checklists, templates, self-assessments, audit logic, trust labels, and certification for full market access.	Data Act Art. 4, 7, 23-24; AI Act Art. 16-21

The modular architecture of the AIGN Framework supports phased adoption—enabling startups, public bodies, and large enterprises to address the most urgent compliance gaps first, then scale up to full certification as capacity grows.

Use Cases & Examples

Use Case 1: Industrial IoT Data Sharing

Scenario:

A European manufacturing consortium needs to share sensor data from connected machines across multiple countries, including partners outside the EU.

Challenge:

- Data must be accessible and portable for all authorized parties (Data Act Art. 4, 23).
- Any AI that analyzes this data (predictive maintenance, supply chain optimization) must document model provenance, data quality, and bias checks (AI Act Art. 10, 13).

AIGN Solution:



The AIGN Data Act Governance Framework 1.0

- The consortium implements the full lifecycle pillar, using AIGN’s tools to map data access rights, create auditable logs, and provide “AI Ready” compliance certifications for each partner.

Use Case 2: Smart Health Platforms

Scenario:

A pan-European telehealth provider uses patient-generated device data for AI-based diagnostics.

Challenge:

- Device and health data must be governed under Data Act, GDPR, and sectoral rules.
- The AI models must be transparent, auditable, and aligned with the EU AI Act’s high-risk provisions.

AIGN Solution:

- Trust & capability indicators are applied to assess and demonstrate system robustness, privacy, and explainability.
- Risk mapping and audit templates ensure compliance across both data and AI lifecycle stages.

Use Case 3: Cross-Border B2B Data Ecosystems

Scenario:

A logistics platform enables data sharing among European and global transport operators, supported by AI-powered route optimization.

Challenge:

- Interoperability and non-discriminatory access are mandated (Data Act Art. 23-24).
- AI transparency and bias mitigation are required (AI Act Art. 13, 16).

AIGN Solution:

- AIGN’s compliance readiness tools and certification labels provide partners with proof of conformity, facilitating faster onboarding and trust in shared digital infrastructure.

Global Perspective



The AIGN Data Act Governance Framework 1.0

- **Alignment with Global Standards:**

The framework is mapped to OECD AI Principles, ISO/IEC 42001, NIST AI RMF, and the Data Governance Act, allowing multinationals to **harmonize governance and compliance worldwide**.

- **Emerging Markets:**

AIGN’s modular structure allows local adaptation for Africa, Asia, and LatAm, where capacity, legal context, and digital maturity vary—but global data and AI integration is rising rapidly.

- **Cross-Border Legal Certainty:**

Companies that operationalize AIGN’s pillars can demonstrate compliance with the strictest regimes—unlocking new markets and public procurement opportunities.

Conclusion & Call to Action

The AIGN EU Data Act AI Governance Framework’s pillar logic ensures that every organization can:

- Replace fragmented compliance and “tick-box” exercises with a unified, value-driven system.
- Prove, not just promise, responsible data and AI practices.
- Achieve continuous readiness—for audits, innovation, and global partnerships.

“A harmonized framework is needed to remove barriers to an effective data economy and ensure fair, secure access to data for all market actors.”



The AIGN Data Act Governance Framework 1.0

Core Pillars vs. Regulation Table

Core Pillars vs. Regulation Mapping Table

The following table provides a direct mapping of the framework’s core pillars to the key requirements of each regulation.

Pillar	Data Act – Key Requirements	AI Act – Key Requirements	DGA – Key Requirements	Example Framework Module / Tool
Trust	Data access rights, contractual fairness (Art. 3–13)	Transparency, explainability (Art. 13–15)	Intermediary trust, data altruism (Art. 11–21)	Trusted Intermediary Toolkit, Consent Mgmt
Maturity	Governance process, continuous improvement (Art. 23)	Risk management systems (Art. 9, 29)	Registration & oversight (Art. 16–17)	Maturity Model, Governance Scorecard
Risk	Data misuse, access security (Art. 24, 33)	High-risk AI management (Art. 8–19)	Intermediary breach prevention (Art. 17, 22)	Risk Register, Incident Response Plan
Compliance	Audit, documentation, reporting (Art. 4, 28)	Technical documentation (Art. 18–19)	Auditability, transparency (Art. 18–19)	Compliance Checklist, Certification Suite

“The table below summarizes how each core pillar aligns with the most relevant articles of the EU Data Act, EU AI Act, and Data Governance Act, providing clear traceability from regulation to operational framework module.”

7. Governance Domains & Lifecycle

Structured Introduction

Modern data- and AI-driven organizations operate in a fast-evolving regulatory landscape. The AIGN EU Data Act AI Governance Framework defines clear **governance domains** and a structured **lifecycle** to ensure compliance, reduce risk, and enable innovation at every stage. This holistic approach breaks down silos and provides operational clarity for roles, processes, and controls—making the entire data and AI journey traceable, auditable, and adaptable.



The AIGN Data Act Governance Framework 1.0

Facts & Data

- **Regulatory convergence:** The EU Data Act, EU AI Act, and Data Governance Act all require organizations to map, document, and govern not just **what** they do with data and AI, but **how** and **why**—with proof, not just intention.
- **70% of compliance breaches** in AI/data projects result from unclear ownership, fragmented documentation, and poorly defined lifecycle processes (EY, 2024).
- **Lifecycle logic** is now embedded in law: The Data Act mandates traceable data access/sharing across B2C, B2B, and B2G (Arts. 3-5, 23); the AI Act requires risk and quality checks at every AI development stage.

Core Governance Domains

Domain	Description & Core Activities	Key Legal References
Data Access, Rights & Contracts	Managing lawful, fair, and transparent access to data for users, third parties, and authorities.	Data Act Art. 3-7, 13, 23; DGA Ch. 3
Data Quality & Provenance	Ensuring data accuracy, lineage, completeness, metadata, and lawful origin for all AI/data uses.	Data Act Art. 23-24; AI Act Art. 10; GDPR Art. 5
Privacy & Security	Embedding privacy (GDPR), security by design, pseudonymization, and confidentiality for all actors.	GDPR; Data Act Art. 7, 8; AI Act Art. 9, 29
AI Model Governance	Documenting training data, model design, risk classification, explainability, oversight, and audit.	AI Act Arts. 10-19; Data Act Art. 24
Interoperability & Portability	Enabling seamless data transfer, standard formats, switching cloud/services, and cross-border access.	Data Act Art. 23-24; DGA Art. 9-12
Incident & Dispute Management	Channels for complaints, redress, dispute resolution, and structured incident escalation (data & AI).	Data Act Art. 33; AI Act Art. 65; DGA Art. 18
Accountability & Documentation	Audit trails, reporting, certification evidence, and documentation of decisions across the lifecycle.	Data Act Art. 3, 4, 13; AI Act Arts. 17, 19

Lifecycle Phases & Activities

1. Data Generation & Collection



The AIGN Data Act Governance Framework 1.0

- Lawful, fair, and transparent collection from IoT devices, users, business sources (Data Act Art. 3).
- Clear pre-contractual info, user rights disclosure (Data Act Art. 3, 4; GDPR Art. 13).

2. Data Access, Sharing & Use

- Rights management for users, partners, authorities (Data Act Art. 4-5, 23).
- Secure, auditable access and non-discriminatory sharing; contractual fairness (Art. 13).

3. Data Quality & Provenance

- Documenting source, quality, and transformation of data; lineage and metadata (Data Act Art. 23, 24).
- Ensuring data meets requirements for lawful AI use (AI Act Art. 10).

4. AI Model Development & Training

- Risk and quality checks on training data (AI Act Art. 10-13).
- Explainability, fairness, bias mitigation, and model documentation.

5. AI Deployment, Monitoring & Auditing

- Continuous oversight: incident detection, explainability, human-in-the-loop logic (AI Act Art. 14-19).
- Monitoring for drift, misuse, new risks, and legal changes.

6. Lifecycle Review & Improvement

- Regular audits, feedback, maturity assessment, recertification (Data Act Art. 24; AI Act Art. 19).
- Updating controls based on incidents, best practice, and new legal obligations.

Use Cases & Examples

Use Case 1: Smart Cities

A European city partners with multiple vendors to deploy smart sensors and AI-powered traffic management.

Framework in action:



The AIGN Data Act Governance Framework 1.0

- Data access/portability enables city authorities and citizens to access and reuse sensor data (Data Act Art. 4, 23).
- Model governance ensures all AI decision-making (e.g. traffic flows) is transparent and auditable (AI Act Art. 13, 14).
- Incident management provides a public channel for citizens to report AI/data errors or harms.

Use Case 2: B2B Data Marketplaces

A cross-sectoral data exchange platform facilitates sharing between SMEs, corporates, and public agencies.

Framework in action:

- Contractual logic guarantees fair, non-discriminatory data access for all participants (Data Act Art. 13).
- Data quality/provenance tools support buyers and sellers in verifying, auditing, and certifying data and AI products.

Use Case 3: High-Risk AI in Healthcare

A hospital develops and deploys a diagnostic AI system trained on European patient data.

Framework in action:

- Training data quality and provenance are fully documented, ensuring legal and ethical compliance (AI Act Art. 10; Data Act Art. 23).
- Privacy, patient rights, and redress mechanisms are integrated via GDPR/Data Act/AI Act cross-mapping.
- Continuous lifecycle review ensures that any incidents, errors, or regulatory changes are quickly addressed.

Adaptation Across Sizes:

SMEs and large enterprises benefit from the same lifecycle logic, but the framework provides tailored checklists and role definitions for different organization types—ensuring relevance and scalability.

Global/Local Application:

Local adaptation is supported through configurable templates and process guidance for specific jurisdictions outside the EU.



The AIGN Data Act Governance Framework 1.0

Global Perspective

- **International readiness:** By structuring the governance lifecycle in line with global best practice (OECD, ISO/IEC 42001, NIST RMF), AIGN enables organizations to “future-proof” their compliance worldwide.
- **Local adaptation:** Emerging economies and local agencies can adapt domains and lifecycle phases to their own capacity, risk, and legal maturity—without losing interoperability with EU and global partners.
- **Public/private value:** The lifecycle logic supports both private sector competitiveness and public sector accountability—ensuring a trustworthy digital society.

“The Data Act... sets out who is entitled to use which data under what conditions, aiming for fair access and legal certainty for all actors.”

8. Data Access & User Rights Management

Management Summary

In the digital economy, fair and secure access to data is not only a regulatory requirement but also a driver of innovation, trust, and competitiveness. The EU Data Act, the Data Governance Act, and the EU AI Act collectively strengthen users’ rights to access, use, share, and manage data generated through connected products and digital services. Effective Data Access & User Rights Management is thus a cornerstone of any certifiable AI governance system. This chapter operationalizes these rights by defining robust technical, organizational, and legal processes for data access, transparency, control, and portability.

Why Data Access & User Rights Management Matter

- **Legal necessity:** The EU Data Act (Articles 4, 13, 23), DGA, and GDPR enshrine user rights to access, export, and erase data, as well as to define and revoke sharing permissions.
- **Trust enabler:** Organizations that make data access transparent and user-centric gain competitive advantage and regulatory resilience.
- **Operational leverage:** Empowering users (B2C, B2B, B2G) to control and monitor their data unlocks business model innovation, reduces compliance risks, and increases engagement.

Key Objectives

- Guarantee that users can access and export their data in a structured, machine-readable, and secure manner.
- Ensure user rights management is audit-ready, transparent, and technically enforceable across the data lifecycle.



The AIGN Data Act Governance Framework 1.0

- Provide clear workflows for granting, managing, and revoking data access and sharing permissions.
- Document all data transfers, user consents, opt-ins/opt-outs, and data deletion actions in compliance with EU law.

9. Mapping Table: Regulatory Requirements to Framework Solutions

Management Summary

Modern AI and data governance cannot exist in a regulatory vacuum. With the EU Data Act, Data Governance Act (DGA), and EU AI Act, organizations face a complex web of compliance duties. This mapping table provides a transparent, actionable bridge between each regulatory requirement and the concrete modules, tools, and processes of the AIGN Data Act AI Governance Framework. It enables organizations, auditors, and stakeholders to trace every legal obligation to its practical fulfillment and provides a one-glance reference for compliance and certification.

Why a Mapping Table?

- **Transparency:** Clarifies which framework module addresses each regulatory requirement.
- **Audit readiness:** Facilitates internal/external review and certification processes.
- **Implementation efficiency:** Supports organizations in identifying gaps, overlaps, and integration points.
- **Continuous improvement:** Serves as a living document to accommodate legal or technical updates.

Table Structure

- **Regulation / Article:** Reference to the specific regulation (Data Act, DGA, AI Act) and its section/article.
- **Obligation / Requirement:** Short description of the legal or operational requirement.
- **Framework Module / Solution:** The AIGN Framework chapter, tool, or process that provides compliance.

Mapping Table



The AIGN Data Act Governance Framework 1.0

Regulation / Article	Obligation / Requirement	Framework Module / Solution
Data Act Art. 4, 13, 23	User data access, export, and deletion rights	Data Access & User Rights Management (Ch. 5.x)
Data Act Art. 23–24	Technical interoperability, API/data export requirements	Technical Reference Architectures & Integration Blueprints (Ch. 30)
Data Act Art. 13	Contractual fairness and non-discrimination	Standard Contract Clauses & Fairness Checklist (Annex/Ch. 35)
DGA Ch. III	Data intermediaries/trustee neutrality, certification	Trusted Data Intermediaries & Data Trustee Models (Ch. 31–33); Audit-Checklists
DGA Ch. V	Data altruism, responsible sharing	Data Altruism & Responsible Sharing (Ch. 32); Documentation Checklist
AI Act Art. 10	Data quality, model provenance, traceability	Data & AI Lifecycle Governance (Ch. 5–7); Documentation Module
AI Act Art. 9, 29, 61	Risk management, monitoring, reporting	Risk & Impact Mapping (Ch. 11); Incident Governance (Ch. 29)
GDPR/AI Act	Explicit consent, lawful basis, opt-in/out	Data Access & User Rights Management (Ch. 5.x); Audit Trail & Logging
All	Documentation, auditability, certification	Assessment Tools & Certification (Ch. 8); Continuous Improvement (Ch. 29)
Data Act/DGA	Stakeholder participation, transparency, feedback	Stakeholder Engagement & Peer Learning (Ch. 28)

Implementation Notes

- **Placement:** This table should be placed immediately after the Key Objectives section.
- **Customization:** Organizations should expand this table to reflect sector-specific or national add-ons as needed.
- **Update frequency:** The mapping should be reviewed and updated regularly (minimum annually or after regulatory changes).



The AIGN Data Act Governance Framework 1.0

- **Certification:** The mapping table serves as a core reference during self-assessments, third-party audits, and certification procedures.

Example Use

When facing an audit or regulatory request, organizations can use this table to:

- Instantly identify where each legal requirement is operationalized.
- Provide direct evidence from the framework (e.g. workflow, policy, tool).
- Demonstrate integration of Data Act, DGA, and AI Act duties in a single, certifiable system.

Core Implementation Requirements

1. **Access & Export Workflows**
 - Users must be able to request, view, and download their data (raw and processed) at any time.
 - Data must be provided in standard, machine-readable formats (e.g. JSON, CSV, XML), with full metadata and time stamps.
 - APIs and self-service portals should facilitate these workflows for all relevant user categories (consumers, businesses, public authorities).
2. **User Rights Management**
 - Every data processing or sharing action requires explicit, documented user consent or legal basis (cf. GDPR Art. 6).
 - Users must be able to manage sharing permissions (granular, revocable, transparent).
 - Opt-out and data erasure (“right to be forgotten”) must be available and technically enforced.
3. **Audit Trail & Logging**
 - All access, export, sharing, and deletion activities must be automatically logged (including user identity, action, data set, timestamp).
 - Logs must be protected against manipulation and be exportable for compliance audits.
 - Regular reviews to detect unauthorized access or unusual activity.
4. **Data Deletion & Retention**
 - Define clear retention periods and automatic deletion rules.
 - Enable users to request full or partial data deletion and ensure proof of erasure.
5. **Transparency & Communication**
 - Provide clear, user-friendly information (in all relevant languages) about which data is collected, how it is used, and users’ rights.
 - Maintain a Data Rights Dashboard for ongoing transparency.

Use Case Example



The AIGN Data Act Governance Framework 1.0

A connected mobility platform allows fleet customers to:

- Download all vehicle usage data in standardized CSV format.
- Grant or revoke data sharing permissions for maintenance partners via an online dashboard.
- View a complete history of data exports and sharing events.
- Request immediate deletion of selected vehicle or user data, with confirmation provided.
- Audit all access and export events via a user-facing activity log.

Compliance & Certification Criteria

- Automated export of user data (in required formats) within statutory deadlines.
- Evidence of technically enforced opt-in/opt-out, sharing, and erasure processes.
- Quarterly internal audits of data access logs and user rights management workflows.
- User feedback mechanism to report access issues or rights violations.
- Integration with Data Intermediary and Data Trustee models (DGA compliance).

Quick Checklist for Implementation

- Are user access/export APIs live and tested for all data categories?
- Is every user action (access, share, delete) fully logged and auditable?
- Can users manage permissions and exercise rights via self-service tools?
- Are deletion and retention rules automated and certified?
- Is information on data rights available, understandable, and multilingual?

Continuous Improvement

- Incorporate user feedback to optimize workflows and remove friction.
- Run periodic privacy and data access “fire drills” to validate readiness.
- Benchmark user rights management against sector best practices and legal developments.



The AIGN Data Act Governance Framework 1.0

Regulatory Mapping Table

This table connects each core requirement from the EU Data Act, EU AI Act, and Data Governance Act (DGA) to the specific AIGN Framework modules, tools, and templates that enable compliance.

Regulation	Key Requirement / Article	Framework Solution / Tool	Compliance Status (✓/~)	Action Needed
EU Data Act	Art. 3–8 (Data access, portability, user rights)	Data Access Management, User Rights Portal	✓	Continuous audit
EU AI Act	Art. 10–19 (Data quality, risk, transparency)	AI Risk Register, Model Cards	✓	Expand documentation
DGA	Art. 12–23 (Intermediaries, altruism, registration)	Intermediary Module, Altruism Toolkit	~	Add more DGA templates

10. Risk & Impact Mapping

Structured Introduction

In the data and AI era, risks are dynamic, interconnected, and extend far beyond technology: they are legal, ethical, operational, and societal.

The EU Data Act, EU AI Act, and Data Governance Act **require organizations to proactively identify, document, and mitigate risks** across the entire data and AI lifecycle—not just for compliance, but to protect users, markets, and society at large.

AIGN’s Risk & Impact Mapping pillar transforms this requirement into operational logic—making risk management measurable, actionable, and certifiable.

Facts & Data

- **Regulatory imperative:**
Both the Data Act (Art. 23-24, Recital 2, 4, 7) and the AI Act (Art. 9, 29; Ch. 2-3)



The AIGN Data Act Governance Framework 1.0

make risk assessment, impact analysis, and mitigation central obligations—especially for high-risk AI, critical data uses, and cross-border operations.

- **Rising complexity:**
Over **80% of organizations** report that their biggest challenge is the identification and management of risks that emerge at the intersection of data sharing, AI, and cloud (Deloitte, 2024).
- **Societal impact:**
Poor risk governance leads to discrimination, privacy breaches, loss of trust, market exclusion, or even regulatory bans—real risks, not theoretical (see: AI failures in healthcare, finance, mobility).

Risk & Impact Mapping Domains

Risk Category	Key Questions & Activities	Legal Reference
Legal & Regulatory	Are all data access, sharing, and AI uses compliant? Are contractual obligations, data rights, and consents clear?	Data Act Art. 4, 13, 23; AI Act Art. 10-19
Technical & Security	Are there vulnerabilities in data collection, sharing, model training, deployment, or interoperability?	Data Act Art. 23-24; AI Act Art. 9, 29
Ethical & Social	Could data or AI decisions cause unfair bias, discrimination, exclusion, or harm to individuals/groups?	AI Act Art. 10, 13; DGA Ch. 3
Operational	Are there risks of business interruption, loss of access, vendor lock-in, or data unavailability?	Data Act Art. 23-24
Societal & Market	Could systemic issues undermine public trust, market access, or social welfare?	Data Act Recital 4; AI Act Recital 3

AIGN Risk Tools & Methodologies

- **Risk Registers:**
Comprehensive templates for logging and updating risks across data and AI projects—mapped to regulatory requirements.
- **Heatmaps & Dashboards:**
Visual tools to identify risk “hotspots” across lifecycle phases, domains, or organizational units.
- **Risk Assessment Checklists:**
Step-by-step guides for regular, auditable risk reviews—covering legal, technical, ethical, and societal aspects.



The AIGN Data Act Governance Framework 1.0

- **Incident Response Mapping:**
Pre-defined escalation matrices and response playbooks for when risk materializes (e.g., data breach, AI malfunction, compliance audit).
- **Stakeholder Impact Analysis:**
Tools to analyze and document how risks may affect users, customers, employees, and society at large.

Use Cases & Examples

Use Case 1: Data Sharing in IoT Ecosystems

Scenario:

A European smart grid operator shares energy usage data with partners for AI-driven optimization.

Risk Mapping:

- Legal: Data access rights, cross-border sharing, consent (Data Act Art. 4, 23).
- Technical: Security risks in device data, interoperability failures.
- Ethical: Potential for discriminatory pricing or exclusion (AI Act Art. 10, 13).
- Societal: Systemic impacts if AI models misallocate resources in vulnerable areas.

AIGN Approach:

A full risk register is maintained, and regular risk reviews are part of operations; red-flagged issues trigger incident response plans.

Use Case 2: High-Risk AI in Finance

Scenario:

A fintech startup uses external datasets and AI for automated credit scoring.

Risk Mapping:

- Legal: Compliance with data source rights, consent, and usage boundaries (Data Act, GDPR).
- Technical: Bias in training data, black-box decisions.
- Ethical: Risk of exclusion/discrimination for certain groups.
- Market: Regulatory investigation or fines for non-compliance.

AIGN Approach:

Automated heatmaps identify high-risk model behavior; dashboards allow management to proactively intervene and document actions for regulators.



The AIGN Data Act Governance Framework 1.0

Use Case 3: Public Sector Data & AI

Scenario:

A government agency leverages shared health data and AI for epidemic prediction.

Risk Mapping:

- Societal: Potential for misallocation of resources, unfair prioritization.
- Privacy: Risk of re-identification in health data.
- Legal: Adherence to sectoral, Data Act, and AI Act rules.
- Operational: Need for rapid, documented incident response if models malfunction.

AIGN Approach:

Stakeholder impact analysis ensures transparent communication and accountability to the public.

Global Perspective

- **Future-proofing compliance:**
The AIGN approach is mapped to global frameworks (OECD AI Principles, ISO/IEC 42001, NIST RMF, Data Governance Act)—allowing organizations to **identify, compare, and mitigate risks globally**.
- **Local adaptation:**
Risk templates and checklists can be tailored to reflect local laws, capacities, and risk appetites—without sacrificing interoperability or global best practice.
- **Building public trust:**
Proactive risk mapping and communication is increasingly demanded by investors, regulators, and civil society—especially for cross-border operations and AI

Supporting Audit and Response:

Structured risk registers and incident mapping not only meet regulatory demands but also empower organizations to prepare for—and respond quickly to—regulatory audits and real-world incidents.



The AIGN Data Act Governance Framework 1.0

Risk Category vs. Regulation Mapping Table

The table below maps all key risk domains addressed in the framework to their corresponding regulatory requirements and the main AIGN risk management tools.

Risk Category	Data Act – Key Reference	AI Act – Key Reference	DGA – Key Reference	AIGN Risk Tool / Module
Data misuse & unauthorized access	Art. 3, 24, 33	Art. 10, 15, 18	Art. 17, 22 (reuse, transfer)	Data Risk Register, Access Controls
Incomplete user consent	Art. 4, 13	Art. 16, 22	Art. 11–14 (consent, transparency)	Consent Audit Trail, User Rights Log
High-risk AI (bias, opacity)		Art. 8–19		AI Risk Heatmap, Model Card Audit
Intermediary breach (DGA)			Art. 17, 22 (intermediary breach, misuse)	Intermediary Risk Assessment Toolkit
Inadequate documentation/audit	Art. 28	Art. 18, 19	Art. 18–19	Audit Trail, Compliance Dashboard
Contractual disputes	Art. 13, 23		Art. 21 (contract fairness)	Standard Clause Review, Risk Reports

“Obstacles to data sharing prevent optimal distribution of data for societal benefit... A harmonized framework must establish who can use data under what conditions.”

11. Compliance & Regulatory Readiness

Structured Introduction

The evolving EU regulatory landscape is setting global benchmarks for data and AI compliance.

The EU Data Act, EU AI Act, GDPR, and Data Governance Act form a complex, interconnected web of obligations for every organization—requiring not just legal awareness, but **operational proof** of compliance across data and AI activities.

AIGN’s Compliance & Regulatory Readiness pillar provides organizations with a **roadmap, tools, and templates** to efficiently and confidently meet these requirements—turning compliance from a cost center into a competitive advantage.

Facts & Data



The AIGN Data Act Governance Framework 1.0

- **Market impact:**
By 2026, more than **80% of EU-based companies** will be directly regulated by the Data Act and AI Act (IDC Europe, 2024).
Over **90% of global B2B contracts** with EU partners will require demonstrable compliance (Forrester, 2024).
- **Consequences of non-compliance:**
Fines under the AI Act can reach up to **€35 million or 7% of annual turnover**; Data Act violations carry strict civil and market penalties, including exclusion from data marketplaces.
- **Regulatory expectation:**
Regulators demand documented, auditable proof—**not** self-attestation. Compliance must be “by design and by default” (GDPR Art. 25; Data Act Recital 7).

Key Compliance Domains & Mapping

Requirement	What's Needed	Reference
Data Access & User Rights	Mechanisms to provide users/partners with access to all relevant data; clear information on rights, contract logic, opt-outs.	Data Act Art. 3, 4, 13; DGA Ch. 3; GDPR Art. 15-20
Contractual Fairness	Standardized, non-abusive B2B/B2C clauses for data sharing, portability, and switching providers.	Data Act Art. 13, 23-24
Documentation & Auditability	Traceable records for all data and AI activities; logs, version histories, model cards, audit trails.	Data Act Art. 23-24; AI Act Art. 17, 19
Risk Classification & Management	Processes for identifying, documenting, and mitigating risk for both data sharing and AI system use.	Data Act Art. 24; AI Act Art. 9, 29
Transparency & Explainability	Easy-to-understand information for users, regulators, and partners about how data and AI systems work.	Data Act Art. 4, 24; AI Act Art. 13, 16
Privacy & Security	Built-in safeguards (privacy by design, security measures, breach notification, data minimization).	Data Act Art. 7, 8; GDPR Art. 25, 32; AI Act Art. 9



The AIGN Data Act Governance Framework 1.0

The AIGN checklists and templates are mapped side-by-side to the requirements of the Data Act, AI Act, and DGA, enabling compliance teams to see at a glance which obligations are covered and where action is needed.

Future-Proof Compliance:

The modular design ensures the framework can be updated as new regulations emerge, protecting investments and reducing long-term compliance costs.

■ AIGN Compliance Tools & Templates

- **Readiness Checklists:**
Self- and external assessment forms, tailored for Data Act and AI Act compliance, covering every lifecycle stage.
- **Certification & Trust Label:**
Third-party attestation and digital badge for partners, regulators, and customers—showcasing maturity and readiness.
- **Contract Templates:**
Pre-vetted data sharing, access, and B2B/B2C contract clauses, mapped to Data Act/AI Act minimum requirements.
- **Audit Trail Templates:**
Standardized documentation for data/AI activities, including data lineage, model documentation, change logs.
- **Incident Reporting Forms:**
Ready-to-use forms for rapid response and regulatory notification (Data Act Art. 33; AI Act Art. 65).

■ Use Cases & Examples

Use Case 1: B2B SaaS Provider

A cloud analytics company wants to sell to EU clients across finance and manufacturing.

Framework in action:

- Implements AIGN readiness checklist and trust label to demonstrate compliance in procurement.
- Uses AIGN contract templates to ensure non-discriminatory data access and switching clauses.
- Maintains audit trails for all client data, enabling rapid response to regulatory requests.



The AIGN Data Act Governance Framework 1.0

Use Case 2: HealthTech Startup

A telemedicine provider integrates wearable data and AI-based recommendations.

Framework in action:

- User dashboards and automated reporting ensure users can access, port, or delete their data (Data Act, GDPR).
- Model documentation and audit templates fulfill AI Act transparency and risk requirements.

Use Case 3: Public Sector Data Collaboration

A city authority joins an EU data space initiative for mobility and energy.

Framework in action:

- AIGN tools streamline Data Act compliance for B2G data provision (Data Act Art. 5).
- Certification supports participation in cross-border, multi-stakeholder projects with shared standards.

Global Perspective

- **Alignment beyond Europe:**
Many global regulations (Brazil LGPD, India DPDP Act, Singapore PDPA, US state laws) are converging toward the EU model; AIGN's compliance logic positions organizations for seamless global operations.
- **Preferred partner status:**
International enterprises increasingly require Data Act/AI Act-style assurance from all partners; AIGN certification is a "passport" to new contracts and markets.
- **Regulator readiness:**
Prepares for emerging regulatory frameworks—ISO/IEC 42001, OECD AI Principles, NIST AI RMF, and more.

"Regulators will expect not just compliance, but auditable, continuous proof... Organizations must build compliance into every step, by design and by default."



The AIGN Data Act Governance Framework 1.0

Compliance Readiness Mapping Table

This table maps regulatory compliance and readiness requirements to corresponding AIGN Framework readiness tools and processes.

Regulation	Compliance Requirement	Framework Readiness Tool / Process	Status (✓/~)	Action Needed
EU Data Act	Documentation, audit, reporting	Compliance Checklist, Audit Trail	✓	Schedule periodic review
EU AI Act	Technical documentation, monitoring	High-Risk AI Compliance Tracker	✓	Add post-market feedback
DGA	Registration, oversight	DGA Readiness Checklist, Registry Log	~	Update registration template

12. Assessment Tools & Certification

Structured Introduction

In the age of regulated data and AI, organizations must **demonstrate** not only intent, but practical, ongoing compliance and trustworthiness.

Assessment tools and certification programs provide a structured, auditable path—moving organizations from “policy on paper” to “proof in practice.”

The AIGN EU Data Act AI Governance Framework makes this operational: with modular tools, ready-to-use templates, and globally recognized trust labels.

Facts & Data

- **Growing demand:**

Over **75% of organizations** cite “demonstrable compliance” as a top factor for partner selection, procurement, and market entry (Forrester, 2024).



The AIGN Data Act Governance Framework 1.0

- **Audit readiness:**
The Data Act and AI Act require organizations to provide documentation, audit trails, and evidence **on demand**—for all regulated data and AI systems (Data Act Art. 23-24; AI Act Art. 17, 19).
- **Certification as trust driver:**
Trust labels and third-party attestation are rapidly becoming prerequisites in B2B and public sector contracts—especially for cross-border, high-risk, or sensitive applications.

Key Assessment Tools

Tool	Purpose	Linked Regulation
AIGN Data & AI Readiness Check	Modular, self- and third-party assessment for Data Act/AI Act maturity at each lifecycle stage	Data Act Art. 3-5, 23; AI Act Art. 9, 17
Compliance & Trust Label	Digital badge/certificate signaling documented, operational compliance to regulators and partners	Data Act Art. 24; AI Act Art. 20, 49
Audit Trail & Documentation Toolkit	Standardized templates for data provenance, model cards, change logs, version control, incident logs	Data Act Art. 23; AI Act Art. 17, 19
Contract & Access Templates	Pre-vetted clauses for data sharing, user rights, interoperability, and risk allocation	Data Act Art. 13, 23-24
Incident Response & Escalation Tools	Structured forms and workflows for incident management, notification, and regulatory reporting	Data Act Art. 33; AI Act Art. 65

Certification Logic & Maturity Model

- **Tiered Certification:**
 - **AIGN Trust Label:** For organizations meeting foundational requirements in data/AI transparency, governance, and risk management.
 - **Sector-Specific Endorsements:** Specialized certifications for finance, health, mobility, public sector, etc.—aligned to sectoral codes and EU requirements.
 - **Engagement Certificate:** For SMEs and early adopters, showing progress toward full compliance and operational best practice.
- **Maturity Model (5 Levels):**



The AIGN Data Act Governance Framework 1.0

1. **Initial:** Ad hoc, undocumented, minimal controls.
2. **Emerging:** Early policies, partial mapping, some templates/checklists in use.
3. **Defined:** Formalized governance, full documentation, audit-ready.
4. **Embedded:** Proactive, continuous monitoring, all processes certified, external attestation.
5. **By Design:** Compliance, risk management, and ethics integrated into every step of business and technology.

Certification Journey Example:

Organizations typically progress from basic self-assessment to full certification within 6–12 months, using AIGN’s tools to close compliance gaps and demonstrate continuous improvement.

Each assessment tool is designed to reduce the time and cost of audits by providing standardized documentation and pre-vetted templates.

Use Cases & Examples

Use Case 1: SME in IoT Manufacturing

Scenario:

A medium-sized manufacturer wants to access EU data marketplaces and supply chains.

AIGN in action:

- Completes a Data & AI Readiness Check, addressing all Data Act and AI Act requirements.
- Earns the AIGN Trust Label, which serves as proof in public and B2B procurement.
- Uses audit toolkits to demonstrate compliance during customer and regulator audits.

Use Case 2: Public Sector Health Authority

Scenario:

A regional health agency participates in a cross-border health data space.

AIGN in action:

- Utilizes audit trail templates to log all data access and AI decisions.
- Achieves sector-specific certification, facilitating interoperability and funding.
- Incident tools enable rapid, compliant response to any breach or data misuse event.



The AIGN Data Act Governance Framework 1.0

Use Case 3: Fintech AI Startup

Scenario:

A startup develops AI models using third-party data for credit scoring.

AIGN in action:

- Applies contract templates to clarify data rights and liabilities with data partners.
- Follows the maturity model roadmap to reach full operational certification within one year.
- Uses incident reporting tools to comply with real-time regulatory notification requirements.

Global Perspective

- **International recognition:**
AIGN's tools and certifications are mapped to OECD AI Principles, ISO/IEC 42001, NIST RMF, and Data Governance Act—providing a single pathway to multi-jurisdictional compliance.
- **Competitive advantage:**
Certified organizations win more contracts, access new markets, and reduce the cost of compliance by standardizing and automating proof.
- **Open, scalable approach:**
The modular toolkit is designed for any organization—from startups to multinationals, public to private, EU and beyond.

“Certification and transparency labels will become critical trust signals for all digital market participants.”

Certification Requirements Mapping Table

This table documents how key certification and audit requirements from each regulation are fulfilled by AIGN's assessment tools and checklists.

Certification Topic	Regulation / Article	Framework Tool / Checklist	Auditability (✓/~)	Notes
Data Access Readiness	Data Act Art. 4–6	Data Access Assessment Checklist	✓	Annual update
High-Risk AI Process	AI Act Art. 14–19	High-Risk AI Self-Assessment	✓	Link to Model Cards



The AIGN Data Act Governance Framework 1.0

Certification Topic	Regulation / Article	Framework Tool / Checklist	Auditability (✓/~)	Notes
Intermediary Registration	DGA Art. 12–17	Intermediary Certification List	~	Add registry link

13. Roles, Responsibilities & Maturity Model

Structured Introduction

A key lesson from regulatory enforcement and real-world AI/data failures: **governance gaps occur when roles and responsibilities are unclear, undocumented, or fragmented.**

Both the EU Data Act and AI Act require organizations to clearly allocate and document **who** is responsible for **what**—across all stages of the data and AI lifecycle.

The AIGN Framework operationalizes this with a RACI-based structure and a continuous maturity model.

Facts & Data

- **Audit findings:**
Over **60% of compliance breaches** result from unclear or overlapping responsibilities, especially in cross-functional and multi-jurisdictional projects (EY, 2024).
- **Regulatory requirement:**
The Data Act and AI Act both specify “documented assignment of responsibilities and accountabilities” (Data Act Art. 3, 4, 13; AI Act Art. 17, 19).
- **Best practice:**
Leading organizations embed role clarity not only for legal reasons, but to accelerate incident response, internal escalation, and continuous improvement.

RACI Model for Data & AI Governance

Role	Description & Typical Responsibilities	Legal Link
Responsible	Executes processes, implements controls (e.g., Data Stewards, AI Developers, Privacy Officers).	Data Act Art. 3, 4; AI Act Art. 17



The AIGN Data Act Governance Framework 1.0

Role	Description & Typical Responsibilities	Legal Link
Accountable	Ultimate decision-maker, ensures overall compliance (e.g., Data/AI Governance Board, CDO, DPO, Board-level Committees).	Data Act Art. 13; AI Act Art. 19
Consulted	Provides expert advice and review (e.g., Legal, Security, Ethics Committee, Works Council).	GDPR, DGA, sectoral rules
Informed	Receives updates, results, key decisions (e.g., Employees, Users, Partners, Public Authorities).	Data Act Art. 4, 23; AI Act Art. 20

How the RACI logic works:

- **Every process** (e.g., data sharing, AI deployment, risk assessment) must have at least one “Responsible” and one “Accountable” person or unit.
- “Consulted” roles bring in required expertise (legal, technical, ethical).
- “Informed” roles guarantee transparency and communication.

RACI in Practice:

In small organizations, the CEO may be Accountable and Data Stewards Responsible; in large enterprises, these roles are distributed across specialized teams.

The maturity model is not only for external certification—it also guides organizations in their internal continuous improvement journey.

Maturity Model

AIGN’s maturity model guides organizations through a **five-level progression**—from ad hoc, reactive governance to fully embedded, proactive, and certifiable excellence.

Level	Key Features
1. Initial	No formal roles or policies; responsibilities undefined; compliance is reactive.
2. Emerging	Some roles assigned; basic documentation; ad hoc compliance responses.
3. Defined	All roles mapped to RACI; responsibilities documented for all lifecycle stages; internal training & onboarding.



The AIGN Data Act Governance Framework 1.0

Level	Key Features
4. Embedded	RACI logic integrated into digital workflows; regular audits, external review, and cross-functional governance boards; rapid escalation processes.
5. By Design	Governance is part of culture; roles, accountability, and improvement logic automated; regular certification; supports innovation and regulatory change.

Use Cases & Examples

Use Case 1: Multinational Cloud Provider

Scenario:

A global SaaS company provides data services to EU clients and must comply with Data Act/AI Act.

AIGN in action:

- Assigns Data Steward for each region (Responsible), Board-level CDO (Accountable).
- Legal, IT Security, and Ethics Committee are regularly Consulted for policy updates and risk reviews.
- All clients and regulators are Informed through dashboards and compliance reports.
- Achieves Level 4 Embedded status in the maturity model, enabling rapid incident escalation and cross-border coordination.

Use Case 2: SME in Mobility

Scenario:

A mobility startup handles mobility data and AI analytics for fleet management.

AIGN in action:

- CEO is Accountable; Data & AI Leads are Responsible; external DPO and legal counsel are Consulted.
- Fleet operators and end-users are Informed through transparent communication channels.
- Moves from Level 2 to Level 3 in the maturity model by formalizing RACI assignments and conducting regular trainings.

Use Case 3: Public Sector Data Collaboration



The AIGN Data Act Governance Framework 1.0

Scenario:

A regional government works with partners in a pan-EU data space.

AIGN in action:

- Clear Responsible and Accountable assignments for data sharing and incident response.
- Consulted roles include privacy authorities and public ethics boards.
- Citizens and the public are Informed via transparency portals.
- Reaches Level 5 By Design maturity, supporting both legal compliance and public trust.

Global Perspective

- **International best practice:**
RACI-based governance is recognized by ISO/IEC 42001, NIST AI RMF, and OECD AI Principles—enabling seamless integration across jurisdictions and sectors.
- **Capacity building:**
The AIGN maturity model provides a structured roadmap for organizations at any starting point—especially valuable for SMEs, emerging markets, and public sector entities.
- **Culture & agility:**
Clear roles and accountability empower organizations to adapt quickly to legal, technological, and market change.

Conclusion & Call to Action

Effective data and AI governance **begins and ends with people.**

Clear roles, shared responsibility, and continuous improvement are the bedrock of trust and resilience.

“Assignment of roles and responsibilities must be documented at every stage... ensuring legal certainty, operational control, and public trust.”

Regulatory Role Mapping Table

This table links framework roles and responsibilities to their regulatory references, ensuring every duty is covered.

Role / Responsibility	Data Act Ref.	AI Act Ref.	DGA Ref.	Framework RACI Link
Data Steward	Art. 4, 23	Art. 10, 16	Art. 12–14	Data Steward



The AIGN Data Act Governance Framework 1.0

Role / Responsibility	Data Act Ref.	AI Act Ref.	DGA Ref.	Framework RACI Link
AI Governance Lead	—	Art. 16–19	—	AI Lead
Data Intermediary Officer	—	—	Art. 12–17	Intermediary
Altruism Manager	—	—	Art. 18–23	Altruism Org

14. Practical Application & Use Cases

Structured Introduction

The true value of any governance framework is proven in real-world application. The AIGN EU Data Act AI Governance Framework has been designed to be practical, adaptable, and scalable—empowering organizations to operationalize compliance, reduce risk, and unlock innovation **across every sector and market**.

Below are key scenarios that illustrate how the framework works in practice—always grounded in the demands of the EU Data Act, EU AI Act, Data Governance Act, and aligned with global best practices.

Key Use Cases

Use Case 1: IoT & Smart Device Ecosystems

Scenario:

A European IoT device manufacturer collaborates with third-party developers and service providers to create a smart home ecosystem.

Application of AIGN Framework:

- **Data Access & Portability:** Ensures device-generated data can be accessed, ported, and reused by end-users and authorized partners in a secure and non-discriminatory way (Data Act Art. 4, 23).
- **AI Model Governance:** All AI-enabled features (e.g., smart assistants, predictive maintenance) are transparently documented and auditable (AI Act Art. 13).
- **Contractual Templates:** Pre-vetted, Data Act-compliant agreements govern partner and user data rights.
- **Outcome:** Faster partner onboarding, reduced legal disputes, and increased customer trust through visible compliance and trust labels.



The AIGN Data Act Governance Framework 1.0

Use Case 2: Cross-Border B2B Data Platforms

Scenario:

A logistics data platform connects freight operators, shippers, and authorities across multiple EU countries.

Application of AIGN Framework:

- **Interoperability:** Data is provided in standardized, machine-readable formats for seamless exchange (Data Act Art. 23-24).
- **Risk Mapping:** Real-time dashboards and risk registers identify and address emerging technical, legal, or market risks.
- **Certification:** Achieving AIGN Trust Label opens new public tenders and private partnerships across borders.
- **Outcome:** The platform becomes the “trusted data intermediary,” increasing participation and revenue.

Use Case 3: Health & Life Sciences

Scenario:

A digital health provider uses patient-generated data and AI diagnostics to offer remote monitoring services.

Application of AIGN Framework:

- **Privacy & Security:** Data collection and AI analytics comply with GDPR, Data Act, and AI Act requirements for sensitive data.
- **Auditability:** All model decisions and data processing are logged and available for audit or regulatory review (Data Act Art. 23; AI Act Art. 17).
- **Redress & Transparency:** Patients have easy-to-use dashboards to access, correct, or delete their data, and to understand AI-generated decisions.
- **Outcome:** High patient trust, successful public sector partnerships, and faster time to market for new features.

Use Case 4: Public Sector Data Spaces

Scenario:

A city government participates in a cross-border mobility data space as part of an EU smart city initiative.



The AIGN Data Act Governance Framework 1.0

Impact: Applying the framework led to faster onboarding, reduced compliance costs, and improved trust signals with stakeholders.

Peer Learning Example:

Organizations reported that participating in incident-sharing led to early detection of similar risks and more effective controls.

Application of AIGN Framework:

- **B2G Data Provision:** Complies with Data Act obligations for providing data to authorities in emergencies or for public interest (Data Act Art. 5).
- **Lifecycle Management:** Regular audits and recertification processes ensure ongoing compliance.
- **Stakeholder Impact:** Transparent public portals show data usage, incidents, and improvements—building citizen trust.
- **Outcome:** Eligibility for EU funding, increased public engagement, and policy innovation.

Additional Application Scenarios

- **Fintech:** AI-driven risk scoring for credit and insurance, with AIGN tools ensuring transparency, bias mitigation, and regulatory readiness.
- **Manufacturing:** Secure, fair data sharing in digital supply chains; audit-proof compliance for OEMs and suppliers.
- **Education:** EdTech providers use AIGN templates to manage student data, enable algorithmic transparency, and participate in European EdTech procurement.

Global Perspective

- **Cross-border compatibility:**
AIGN-certified organizations gain a reputation for reliability in international consortia, joint ventures, and digital trade agreements.
- **Emerging markets:**
Framework modules can be localized—allowing startups and public agencies in Africa, Asia, or Latin America to “plug into” trusted global data and AI spaces.
- **Public sector leadership:**
Governments using AIGN accelerate digital transformation and set standards for private sector partners.

Conclusion & Call to Action

The AIGN Framework’s strength is its real-world impact—enabling organizations to:

- Enter new markets with confidence,



The AIGN Data Act Governance Framework 1.0

- Build trust with every stakeholder,
- Unlock value from data and AI—without sacrificing compliance or ethics.

“Data holders must provide data to users and authorized third parties under fair, reasonable, and non-discriminatory terms... enabling new business models, public interest services, and innovation.”

Use Case to Regulation Mapping Table

This table maps key use cases to the regulatory requirements and the matching AIGN Framework solutions.

Use Case	Regulation(s)	Compliance Requirement	Framework Tool / Template
IoT Device Data Sharing	Data Act, DGA	Data access, user rights	Data Access Portal
Health AI Model Deployment	AI Act, Data Act	Data quality, explainability	Model Card, Data Lineage
Data Intermediary Ecosystem	DGA	Registration, contracts	Intermediary Agreement

15. Integration with International Standards

Structured Introduction

Data and AI do not recognize borders.

To unlock their full potential—and ensure compliance, interoperability, and trust—organizations must align with international frameworks and standards.

The AIGN EU Data Act AI Governance Framework is specifically designed to bridge EU regulation (Data Act, AI Act, DGA, GDPR) with global best practice, enabling organizations to operate seamlessly across markets, sectors, and legal regimes.

Facts & Data

- **Standard convergence:**
Over **120 countries** are developing or adopting AI/data governance regulations.
International bodies—OECD, ISO, NIST, UNESCO—are driving alignment.



The AIGN Data Act Governance Framework 1.0

- **Procurement and market access:**
85% of cross-border tenders for digital/data/AI services now reference at least one international standard, alongside local/EU law (World Bank, 2024).
- **Interoperability as requirement:**
The EU Data Act (Art. 23-24) and DGA demand not only compliance, but **technical and organizational interoperability** with other regimes.

Key Standards & Regulatory Mapping

Standard/Framework	AIGN Mapping / Interoperability	Reference
OECD AI Principles	Core pillars (transparency, accountability, human-centered values) mapped to AIGN trust/capability, risk, and lifecycle domains.	OECD (2019)
ISO/IEC 42001	Management system structure (policies, roles, audits, continual improvement) embedded in AIGN maturity model and RACI logic.	ISO/IEC 42001:2023
NIST AI Risk Management	Risk mapping, impact assessment, documentation, and continuous monitoring—fully aligned with AIGN risk & compliance tools.	NIST AI RMF (2023)
Data Governance Act (DGA)	Trusted data intermediaries, data altruism, and cross-border sharing requirements operationalized in AIGN's data access/contract modules.	EU DGA, Ch. 3, 5
GDPR / Privacy Laws	Data minimization, lawful basis, rights management, breach notification—built into all AIGN pillars and templates.	GDPR (2016), global equivalents
UNESCO AI Ethics	Ethical alignment, impact on society, and sustainability embedded in AIGN's use case and risk domains.	UNESCO (2021)

Bridging Global Gaps:

The AIGN Framework provides step-by-step onboarding for organizations outside the EU, helping them align with EU standards while maintaining compatibility with local regulations (e.g., US, Brazil, India).



The AIGN Data Act Governance Framework 1.0

Example: A US-based healthtech firm used AIGN tools to quickly map their compliance posture for both HIPAA and EU Data Act/AI Act, enabling market entry and joint ventures in Europe.

Use Cases & Examples

Use Case 1: Multinational Data Marketplace

Scenario:

A pan-European data platform enables energy, mobility, and finance companies to exchange data across EU and non-EU borders.

Framework in action:

- Uses AIGN contract templates and audit tools mapped to Data Act, ISO/IEC 42001, and OECD Principles.
- Achieves both EU and global certifications, unlocking B2B and public sector contracts from Finland to South Korea.
- Interoperability features ensure seamless data portability and lawful access for all users.

Use Case 2: International EdTech Platform

Scenario:

A global EdTech company must comply with GDPR in Europe, Brazil's LGPD, US FERPA, and the OECD AI Principles.

Framework in action:

- AIGN maturity model ensures management and audit logic are harmonized across all standards.
- Privacy and explainability templates enable rapid adaptation to new local requirements.
- Certification accelerates onboarding in new markets and cross-border collaborations.

Use Case 3: Cross-Border Smart City Initiatives

Scenario:

EU, African, and Asian cities join forces on AI-powered mobility and environmental services.

Framework in action:



The AIGN Data Act Governance Framework 1.0

- AIGN’s alignment with UNESCO AI Ethics and OECD Principles ensures shared values and impact assessment.
- Data Governance Act and Data Act modules enable trusted sharing and data altruism across jurisdictions.
- Public trust and funding eligibility are enhanced through multi-standard certification.

Global Perspective

- **“One framework, many markets:”**
Organizations using AIGN can map every pillar, policy, and tool directly to international and local standards—creating a single “compliance backbone” for the digital economy.
- **Future-proofing:**
As new laws (e.g., US AI Bill of Rights, India DPDP Act) emerge, the AIGN framework evolves to ensure continued compatibility and global market access.
- **Level playing field:**
Harmonization enables SMEs and public sector agencies to participate in international projects on equal terms with large corporates.

Conclusion & Call to Action

Integration with international standards is not a luxury—it’s a necessity for trust, innovation, and growth.

AIGN empowers organizations to:

- Build systems and partnerships that “work everywhere,”
- Prove readiness for any regulatory, contractual, or ethical review,
- Participate in the global data and AI economy—without redundancy or friction.

“The AIGN Framework is designed as a universal bridge—translating legal requirements, ethical principles, and technical standards into operational reality.”

International Standards Mapping Table

This table shows how the AIGN Framework aligns with international and EU regulatory standards.

Standard / Regulation	Core Principle / Article	Framework Alignment	Status (✓/~)	Notes
ISO/IEC 42001	AI Governance	Full process mapping	✓	Annual review
OECD AI Principles	Fairness, Transparency	Included in Pillars/Tools	✓	Peer learning module



The AIGN Data Act Governance Framework 1.0

Standard / Regulation	Core Principle / Article	Framework Alignment	Status (✓/~)	Notes
EU Data Act / DGA	Data access, intermediaries	Covered in all modules	✓	Add crosswalk table

16. Data & AI Literacy – Empowering Compliance, Trust, and Innovation

Structured Introduction

Data and AI literacy are now critical enablers for regulatory compliance, operational excellence, and digital transformation. Both the EU Data Act and AI Act explicitly recognize that without the right skills, awareness, and culture, governance cannot succeed. The AIGN Framework embeds Data & AI Literacy as a core pillar—moving beyond policies to real capabilities at every level.

Facts & Data

- Over 70% of data protection and AI-related incidents in organizations stem from a lack of data or AI understanding among staff and stakeholders (Deloitte, 2024).
- The EU Data Act requires organizations to inform and empower users and employees on their data rights, sharing, and access possibilities (Art. 3; Recitals 19, 20).
- The EU AI Act mandates AI literacy for all personnel involved in the operation and oversight of AI systems (Arts. 4, 16, 17, 19).
- Leading organizations with formal literacy programs report up to 50% faster compliance processes and 35% fewer security incidents (McKinsey, 2024).

Key Components & Tools

- **Data & AI Literacy Program:** Structured, certifiable training modules—mandatory for certification and continuous improvement cycles.
- **KPI Monitoring:** Track progress with metrics such as share of employees trained, assessment pass rates, and incident reductions.
- **Best Practice Library:** Curated international examples of effective data and AI literacy initiatives, tailored by sector and risk profile.
- **Onboarding & Awareness Kits:** Specialized onboarding content for new roles, AI users, and interface positions—including coverage of ethical risks, bias, and data/AI safety.



The AIGN Data Act Governance Framework 1.0

- **AI System “Red Flag” Awareness:** Practical guides for early detection of AI or data governance issues by non-experts.

Role-based Training:

Technical staff receive advanced AI/data management modules; non-technical and managerial staff complete foundational training.

Regulatory Link

- EU Data Act Art. 3, 4; Recitals 19–20
- EU AI Act Art. 4, 16, 17, 19

Use Cases

- **Healthcare:** Hospitals implement certified AI/data literacy programs for all staff using diagnostic AI tools, reducing misdiagnosis and compliance risk.
- **Manufacturing:** IoT device operators receive targeted training on data rights and sharing under the Data Act, enabling secure, compliant B2B collaboration.
- **Public Sector:** City administrations roll out awareness campaigns for citizens and employees on their data access and control rights, boosting trust and uptake.

Global Perspective

- **Cross-border Compliance:** Data and AI literacy standards are rapidly converging internationally (OECD, UNESCO, ISO/IEC 42001).
- **Emerging Markets:** Scalable modules enable rapid upskilling in local languages and legal contexts, ensuring “no one is left behind.”

17. Data Altruism & Responsible Data Sharing

Structured Introduction

The Data Governance Act (DGA) and Data Act introduce the concept of data altruism: making data available for societal, research, or innovation purposes in the public interest. The AIGN Framework operationalizes data altruism and responsible sharing as an integrated, auditable process.

Facts & Data



The AIGN Data Act Governance Framework 1.0

- Less than 15% of organizations currently enable compliant, purpose-driven data sharing for research, non-profit, or public interest (IDC Europe, 2024).
- Data altruism is set to become a requirement for access to public funding, data spaces, and international research consortia.
- The DGA establishes formal criteria and governance for recognized data altruism organizations and data intermediaries.

Core Elements & Tools

- **Altruism Policy Templates:** Pre-vetted templates for designing, documenting, and publishing data altruism policies and user consent mechanisms.
- **Data Donation Workflow:** Auditable processes for vetting, approving, and monitoring data sharing with external partners or public interest projects.
- **Altruism Registry Integration:** Seamless links to national and EU data altruism registries for certification and transparency.
- **Impact Assessment:** Tools to assess and document the potential societal benefits, risks, and privacy implications of data sharing.

Operationalizing Data Altruism:

Stepwise process: 1) Policy creation; 2) Consent management; 3) Data donation workflow; 4) Registration and impact assessment.

Regulatory Link

- EU Data Governance Act (DGA), Ch. 3, 5
- EU Data Act Art. 5, Recitals 2, 4

Use Cases

- **Smart Cities:** Sharing anonymized mobility data with public health researchers to improve urban planning and epidemic response.
- **Healthcare:** Hospitals contribute anonymized patient data to certified research initiatives, accelerating disease understanding while protecting privacy.
- **Education:** EdTech platforms enable students to opt-in to data sharing for educational research and evidence-based policy.

Global Perspective

- **International Interoperability:** Altruism modules are mapped to global data sharing frameworks (OECD, UNESCO), supporting participation in multi-national data spaces.
- **Responsible Innovation:** Promotes public trust and social license for data-driven business models.



The AIGN Data Act Governance Framework 1.0

Conclusion & Call to Action

Responsible data sharing and data altruism move compliance beyond risk avoidance—positioning organizations as leaders in digital responsibility and public value creation.

18. Peer Learning, Incident Sharing & Continuous Improvement

Structured Introduction

True governance evolves through transparency, peer learning, and continuous feedback—not just rules. The AIGN Framework embeds structured peer-learning and incident sharing to accelerate learning and improve risk resilience across the network.

Facts & Data

- Organizations with active incident-sharing and peer-learning mechanisms recover from data/AI failures 3x faster (Gartner, 2024).
- 60% of compliance errors are repeated because lessons from other organizations are not shared or institutionalized.

Core Elements & Tools

- **Case Library:** Anonymized, regularly updated database of real-world best practices and incidents from across all sectors and regions.
- **Peer Review & Benchmarking:** Interactive platform for organizations to share challenges, seek feedback, and benchmark governance maturity.
- **Mentorship Matching:** On-demand access to AIGN-certified mentors for critical incidents, audits, or implementation challenges.
- **Continuous Improvement Loop:** Structured processes for integrating lessons learned into policies, training, and audits.

For SMEs: Use the “plug-and-play” data lineage template to connect CRM/ERP systems directly to governance reporting tools, meeting Data Act traceability requirements with minimal custom development.

Regulatory Link

- Supported by continuous improvement requirements in ISO/IEC 42001, NIST AI RMF, and best practice governance codes.

Use Cases



The AIGN Data Act Governance Framework 1.0

- **Finance:** A bank shares a near-miss incident via the AIGN Case Library, enabling others to improve their fraud detection processes.
- **SMEs:** Startups participate in peer benchmarking, gaining rapid insight into cost-effective, high-impact governance controls.
- **Public Sector:** Government agencies share lessons from cross-border data collaborations, accelerating policy adaptation.

Global Perspective

- **Scalable Globally:** Tools are accessible to all AIGN members and partners—accelerating improvement in high- and low-resource settings.
- **Regulatory Recognition:** Participation in peer-learning networks is increasingly seen as a sign of proactive, responsible governance.

Conclusion & Call to Action

Peer learning and structured incident sharing are not optional—they are essential accelerators of resilience and excellence in data and AI governance.

19. Technical Reference Architectures & Integration Blueprints

Structured Introduction

Operational governance is only effective when it is technically embedded. The AIGN Framework offers reference architectures and integration blueprints to bridge the gap between compliance, IT, and data/AI engineering.

Facts & Data

- Over 60% of audit failures are caused by missing or incompatible technical controls (Gartner, 2024).
- The Data Act and AI Act increasingly require auditable data lineage, standardized APIs, and technical interoperability.

Core Elements & Tools

- **Reference Architecture Diagrams:** Blueprint examples for compliant data/AI pipelines, lineage tracking, API management, and data/AI interoperability.



The AIGN Data Act Governance Framework 1.0

- **Integration Playbooks:** Step-by-step guides for connecting governance tools with enterprise IT (ERP, CRM, Cloud, Data Lakes).
- **Lineage & Metadata Tools:** Modular templates and code snippets for data/AI lineage capture, logging, and reporting.
- **Cloud & Data Space Integration:** Best practices for cross-border, multi-cloud compliance and participation in EU data spaces.

Regulatory Link

- EU Data Act Art. 23–24; DGA
- AI Act Art. 10 (Data and Record Keeping), Art. 17 (Technical Documentation)

Use Cases

- **Enterprise:** Large companies integrate AIGN governance modules into SAP or Microsoft Azure environments, ensuring end-to-end compliance.
- **SMEs:** Startups leverage plug-and-play blueprints to join B2B data marketplaces without heavy consulting.
- **Data Spaces:** Organizations participate in European or global data spaces, enabled by technical interoperability modules.

Global Perspective

- **International Standards:** Architectures and playbooks map to ISO/IEC 42001, NIST, and major cloud platforms.
- **Local Adaptation:** Blueprints are modular and configurable for any scale or region.

Licensing & Integration:

All interoperability audit templates, interface checklists, and migration test packs can be licensed separately or bundled with technical onboarding packages.
Includes annual updates and community best practice sharing.

20. Trusted Data Intermediaries & Data Trustee Models (DGA Integration)



The AIGN Data Act Governance Framework 1.0

Structured Introduction:

The Data Governance Act (DGA) introduces Trusted Data Intermediaries—regulated, neutral entities facilitating fair, secure, and compliant data sharing across organizations, public bodies, and individuals. These intermediaries are foundational for future European data spaces and collaborative AI ecosystems.

Facts & Data:

- DGA Chapters II-III: Defines data intermediaries, mandates registration, and sets strict requirements for neutrality, security, contractual fairness, and transparency.
- Mandatory registration and regulatory oversight for intermediaries across all EU Member States from September 2025.
- Pioneering model for similar initiatives in India, Japan, Singapore, and beyond.

Key Features & Deliverables:

- Full implementation and evidence of neutrality and independence (no use of data for own purposes).
- Technical and organizational controls for secure data rooms, platforms, and sharing services (secure processing environments, encryption, access controls).
- Documentation and auditability of all intermediary services (transparency obligations under DGA Arts. 11–15).
- Certification and trust labels for registered data intermediaries.

Use Cases:

- **Industry Consortium:** Competing manufacturers use a neutral data trustee for B2B data sharing—reducing antitrust and confidentiality risks.
- **Health Data Space:** Patients channel their data via a certified intermediary to approved research projects.

Global Perspective:

- Trusted intermediary status is becoming a global norm for responsible, sector-spanning data innovation.
- Key for legal certainty and scalable, cross-border data/AI ecosystems.

Conclusion & Call to Action:

Any future-ready data ecosystem must integrate a compliant, neutral intermediary function—operationalized through AIGN modules and certification.

Tool Licensing Note:

The Data Intermediary Audit Kit—including registration checklists, neutrality audit



The AIGN Data Act Governance Framework 1.0

templates, and incident reporting tools—is available for licensing as an add-on module. Annual updates and sector-specific versions can be provided upon request.

21. Data Altruism & Responsible Data Sharing (DGA Integration)

Structured Introduction:

The DGA for the first time creates a legal foundation for voluntary, nonprofit-oriented data sharing (“data altruism”), e.g., in health, research, or sustainability.

Facts & Data:

- Registration and supervision of recognized data altruism organizations (DGA Arts. 16–22).
- EU-wide consent management and withdrawal form.
- Data altruism kept strictly separate from commercial data brokerage.

Key Features & Deliverables:

- User-centric consent management (incl. opt-in, withdrawal, and transparency mechanisms).
- Technical measures: Secure processing environments, audit trails, and anonymization/pseudonymization as required.
- Governance: Ethics board, compliance processes, transparency for contributors.
- Community engagement: Regular reporting to individuals about how their data is used and its societal impact.

Licensing Option:

Data Altruism Readiness Checklists, consent templates, and public reporting dashboards are part of the AIGN Compliance Toolbox and can be licensed for individual or enterprise use. Contact us for tailored versions for health, smart city, or research applications.

Use Cases:

- **HealthTech:** Citizens donate health data to certified platforms for AI-driven research, fully protected by DGA requirements.
- **Climate Data Space:** Companies voluntarily share non-personal environmental data for climate modeling and AI-based sustainability solutions.

Global Perspective:



The AIGN Data Act Governance Framework 1.0

- Data altruism is attracting global attention as a model for data-driven research and “AI for Good.”
- Builds trust and unlocks new, non-commercial data sources.

Conclusion & Call to Action:

Data altruism must be a core compliance and innovation pillar. AIGN provides templates, toolkits, and consent logic to operationalize it.

Tool Licensing Note:

The Data Intermediary Audit Kit—including registration checklists, neutrality audit templates, and incident reporting tools—is available for licensing as an add-on module. Annual updates and sector-specific versions can be provided upon request.

22. Registration, Oversight & Certification of Data Intermediaries (DGA Integration)

Structured Introduction:

The DGA mandates the registration, ongoing oversight, and certification of data intermediaries and data altruism organizations, ensuring public trust and continuous compliance.

Facts & Data:

- Centralized registration across all EU countries (DGA Arts. 10, 19, 20).
- Oversight authorities for data intermediaries and altruism (with enforcement and sanctioning powers).

Key Features & Deliverables:

- AIGN templates for registration, notification, and compliance reporting.
- End-to-end monitoring, auditing, and incident response (breach notification, audit trails).
- Digital certificates/trust labels for compliant intermediaries and altruistic organizations.

Use Cases:

- **B2B Data Marketplace:** Uses AIGN certification to demonstrate compliance and win new data partners.



The AIGN Data Act Governance Framework 1.0

- **Non-profit Research Organization:** Gains EU trust label and preferred status for public AI projects.

Global Perspective:

- Certified intermediaries become preferred partners in international projects, much like ISO/IEC certifications.
- Regulatory convergence and mutual recognition are accelerating worldwide.

Conclusion & Call to Action:

AIGN enables easy adoption of DGA registration, oversight, and certification logic—empowering trusted data ecosystems and facilitating global market entry.

Tool Licensing Note:

The Data Intermediary Audit Kit—including registration checklists, neutrality audit templates, and incident reporting tools—is available for licensing as an add-on module. Annual updates and sector-specific versions can be provided upon request.

23. Technical and Organizational Requirements for Secure Data Environments (DGA/DA Integration)

Structured Introduction:

DGA and Data Act require “secure processing environments” for the sharing and re-use of sensitive or confidential data by intermediaries and users.

Facts & Data:

- DGA/DA Arts. 5, 7, 23: Demand encryption, granular access control, privacy-by-design, anti-reidentification, and full auditability.
- Obligatory for any processing of commercially or personally sensitive data.

Key Features & Deliverables:

- AIGN blueprints for secure data rooms, API architectures, and advanced analytics platforms.
- Controls for ex-post auditing, incident management, and data masking.
- Comprehensive documentation and compliance evidence toolkits.



The AIGN Data Act Governance Framework 1.0

Use Cases:

- **Insurance Platform:** Shares sensitive customer data with AI vendors only within certified secure environments.
- **Research Institution:** Uses AIGN “Data Room” blueprint to enable compliant cross-border data sharing.

Global Perspective:

- Secure data environments are becoming a minimum global standard (e.g., USA, Japan, OECD).
- Prerequisite for cross-border collaboration and AI development.

Conclusion & Call to Action:

No sustainable data or AI ecosystem without secure, auditable data environments—AIGN delivers technical and organizational building blocks for compliance.

24. Stakeholder Engagement, Transparency & Dispute Resolution (DGA/DA Integration)

Structured Introduction:

DGA emphasizes stakeholder engagement, transparency, and structured dispute resolution to foster trust and long-term participation in data ecosystems.

Facts & Data:

- Establishment of information points, transparency obligations, and effective redress mechanisms (DGA Art. 8, 18).
- Mandated communication channels, complaints procedures, and governance transparency for all actors.

Key Features & Deliverables:

- AIGN templates for stakeholder communication and transparency dashboards.
- Standardized processes for feedback, whistleblowing, and redress mechanisms.
- Integration of dispute resolution into the governance framework, including escalation paths.



The AIGN Data Act Governance Framework 1.0

Use Cases:

- **SME:** Gains clarity on data flows, rights, and dispute resolution via AIGN transparency dashboards.
- **Data Space Operator:** Uses standardized complaints and redress processes to build user trust and mitigate regulatory risk.

Global Perspective:

- Stakeholder engagement and transparency are rapidly becoming global benchmarks for data/AI governance and market acceptance.

Conclusion & Call to Action:

Transparency and active stakeholder management are not “nice to have”—they are regulatory and market essentials. AIGN provides the operational toolkit.

Summary for Implementation

- Each new module can be integrated as an individual chapter (Chapters 12–17 or as needed) or as dedicated sub-sections within existing framework domains.
- All new sections strictly follow the AIGN schema for clarity, traceability, and practical usability.
- These additions ensure full DGA coverage—especially for data intermediaries, altruism, secure environments, and stakeholder requirements.

25. Contractual Fairness & Standard Clauses Module

Management Summary

Ensuring fair, transparent, and non-discriminatory contracts for data access and data sharing is a cornerstone of the EU Data Act and essential for trustworthy AI and data governance. Many legal disputes and compliance failures arise from unclear or unbalanced contractual terms—especially regarding rights, obligations, and liabilities around data. This module provides a practical toolkit for contractual fairness, featuring standard clause templates, review checklists, and implementation guidance, enabling organizations to comply with Data Act requirements (especially Articles 13, 23, and 24) and to foster trusted data ecosystems.

Why Contractual Fairness Matters

- **Regulatory imperative:** The EU Data Act prohibits unfair, opaque, or discriminatory contract terms in data access and sharing relationships.



The AIGN Data Act

Governance Framework 1.0

- **Risk mitigation:** Fair contracts reduce litigation, regulatory penalties, and reputational risk.
- **Business enabler:** Transparent and balanced agreements facilitate smoother data collaboration, build trust with partners, and support data-driven innovation.

Key Objectives

- Provide organizations with ready-to-use, Data Act-compliant standard contract clauses.
- Enable easy internal review of contractual fairness, non-discrimination, and transparency.
- Ensure all relevant stakeholders (B2B, B2C, B2G) can understand and exercise their rights.
- Embed contractual auditability and documentation in the data sharing lifecycle.

Core Implementation Requirements

1. **Standard Contract Clause Templates**
 - Templates for data access agreements, data sharing, and data portability.
 - Clear language on user rights, access scope, technical and organizational security, dispute resolution, liability, and exit scenarios.
 - Clauses addressing: opt-in/opt-out, duration, revocation, data deletion, and retention policies.
2. **Fairness Review Checklist**
 - Pre-signing checklist for evaluating contracts: Are all parties' rights/obligations clearly stated? Are data use purposes transparent? Is data usage non-exclusive and non-discriminatory?
 - Checklist items: prohibition of lock-in effects, clear exit terms, data return procedures, no hidden fees, and transparency of all data flows.
3. **Non-Discrimination & Transparency**
 - Ensure that no clause disproportionately favors one party, restricts competition, or limits users' statutory rights.
 - Require clear explanations of fee structures, access procedures, and dispute resolution mechanisms.
 - For SMEs/startups: templates are adapted to minimize legal overhead.
4. **Contract Auditability**
 - All contracts must be logged and versioned (digitally signed where possible).
 - Documentation of contract negotiations, amendments, and user consents.
 - Contracts should be retrievable for audit and regulatory review.
5. **Continuous Update Mechanism**
 - Annual review and update of standard templates and checklists based on legal, sectoral, or technical changes.
 - Feedback mechanism for partners and users to report contractual issues or suggest improvements.



The AIGN Data Act Governance Framework 1.0

Use Case Example

A B2B data-sharing platform onboards a new logistics partner:

- Both parties use the AIGN Standard Data Sharing Agreement, which details mutual rights, access methods, data use limitations, and clear opt-out/termination clauses.
- The platform's contract review tool auto-checks the agreement against the Fairness Checklist.
- In case of dispute, both parties can refer to the transparent contract record and its embedded audit trail.

Compliance & Certification Criteria

- Use of standard, Data Act-aligned contract templates for all relevant data sharing relationships.
- Fairness checklist completed and logged for every signed contract.
- All parties have access to and understanding of contract terms (multilingual support as required).
- Contracts and reviews stored and accessible for internal and regulatory audits.
- Regular internal/external audits on contract fairness and compliance.

Quick Checklist for Implementation

- Are Data Act-compliant standard contract templates in place and up-to-date?
- Is every data access or sharing contract reviewed with a fairness checklist before signing?
- Are all key clauses (access, exit, rights, deletion, liability) included and clear?
- Are contracts versioned, signed, and stored for audit/review?
- Are contract processes updated annually and open to feedback?

Continuous Improvement

- Monitor feedback from partners, users, and auditors to adapt templates and review processes.
- Benchmark contract templates and processes against sectoral best practices and evolving regulation.

Template Licensing:

Standard contract clauses, fairness checklists, and review workflows are available as ready-to-use templates, with annual legal updates.

License as a stand-alone toolkit or as part of your organization's AIGN compliance license.

26. Framework Governance, Usage and Licensing



The AIGN Data Act

Governance Framework 1.0

Legal Structure and Intellectual Ownership

The AIGN Framework, including all its concepts, structures, tools, certification logic, terminology, and visual indicators, is the **intellectual property of AIGN – Artificial Intelligence Governance Network**, represented by its founder **Patrick Upmann**, unless otherwise noted.

The framework has been made publicly accessible in line with AIGN’s mission to promote responsible AI governance globally. However, such accessibility does not imply a waiver of ownership, licensing rights, or brand control.

All rights not explicitly granted herein remain reserved.

Licensing Model

- **Commercial Use, Certification, Partnerships:**
All commercial applications of the AIGN Framework—including use of certification labels, trust badges, tools, templates, and maturity models—require a valid AIGN license and/or partnership agreement.
 - Only certified AIGN partners may offer assessments, certification services, or apply the AIGN Trust Label or derivative marks.
 - Commercial consulting, resale, or integration into products/platforms is only permitted via formal license.
- **Open Access:**
The AIGN Framework is freely accessible for non-commercial educational, academic, and public sector use, provided that no commercial certification, rebranding, or resale occurs.
 - Public authorities and educational/research institutions may use the framework internally or in pilot projects (with attribution).
- **No Commercial Re-Branding:**
Any attempt to rebrand, white-label, or claim derivative works as independent solutions without written AIGN approval is strictly prohibited.

Intellectual Property Protection

- **Comprehensive IP Rights:**
All key components—Trust Label, Education Trust Label, Agentic AI Badge, templates, assessment tools, certification logic, and maturity models—are the intellectual property of AIGN – Artificial Intelligence Governance Network.
 - Use of proprietary logic, methods, and badges is strictly controlled via license; annual audits and integrity reviews are conducted for all partners.



The AIGN Data Act Governance Framework 1.0

- **Scope of Protection:**

Any commercial or public use of the above (including visual design, terminology, process logic, and derivative works) is subject to IP protection and legal enforcement by AIGN.

Compliance & Governance Assurance

- **Attribution:**

All users must provide visible attribution (“Based on the AIGN Framework for Responsible AI Governance, www.aign.global. All rights reserved.”) in any use, document, or training.

- **Partner Agreement:**

Only approved partners, having completed mandatory onboarding and training, are authorized to use AIGN certification logic, tools, and badges in client projects.

- **Audit Mechanisms:**

Regular audits, annual reviews, and integrity checks ensure compliance with AIGN standards and prevent misuse or dilution of trust marks.

Recommendation for International Rollout

To support international adoption and clarity:

- Add a **Licensing Quick Guide** (1-pager):

Explains at a glance: what is freely usable, what is license-protected, and how to become a certified partner.

- Include a **visual overview** (infographic/table) of all protected modules—Trust Label, templates, badges, certification logic, assessment tools, maturity model.
- Provide downloadable resources and a “How to License” FAQ on the website and in framework documentation (ideally before the legal fine print).



The AIGN Data Act Governance Framework 1.0

Sample Visual for the Licensing Quick Guide:

Module/Asset	Open Access	Requires License/Partner
Framework (Reading)	✓	
Internal Non-Commercial Use (Edu/Gov)	✓	
Templates & Tools (Commercial)		✓
Certification / Trust Label		✓
Badges (Education, Agentic AI)		✓
Custom Integrations		✓
Derivative Works / Rebranding		✓

Permitted Uses (Open Access – Non-Commercial)

AIGN permits the use of the AIGN Framework under the following conditions:

- **Copyright & License Policy:**

Clarify that all commercial and non-commercial uses of the AIGN Framework and any AIGN-certified models require documentation of copyright compliance (including model/data provenance and rights reservations).

- Explicitly require that all model providers disclose license types (open/proprietary/restricted) and maintain up-to-date records for audit.

Permitted:

- **Internal application** within organizations for self-assessment, risk identification, and capacity building
- **Academic and educational use** in non-commercial settings, including research and teaching



The AIGN Data Act Governance Framework 1.0

- **Policy analysis** or inclusion in public sector initiatives for non-commercial, public interest purposes
- **Non-commercial referencing**, provided **proper attribution** is given (see 13.5)

Not permitted without prior written agreement:

- Commercial certification or use of AIGN labels, seals, or trust marks
- Sale, sublicensing, or commercial hosting of AIGN tools or methodologies
- White-labeling, rebranding, or claiming derivative ownership
- Misrepresentation of affiliation with AIGN

Protected Elements (Use Requires License or Partnership)

The following components of the AIGN Framework are **protected assets**, and their use is explicitly reserved:

Element	Protection Status
AIGN Global Trust Label	Certification and mark protected by AIGN
Education Trust Label	Requires evaluation and approval by AIGN
Agentic AI Verified Badge	Reserved for certified assessments of agentic systems
Trust Scan, ARAT, Risk Heatmap	Proprietary tools under controlled license
Governance Maturity Model & Capability Indicators	Licensed only for public application, audits, or consulting

These may only be issued, applied, or displayed by **AIGN itself or licensed partners**.

Commercial Use & Derivative Works

Any **commercial use, consulting, resale, adaptation, or public deployment** of the AIGN Framework in whole or in part requires:

1. A formal **AIGN Partner Agreement**
2. A valid **AIGN License** for the intended purpose
3. Adherence to **quality assurance and integrity standards** defined by AIGN
4. Clear distinction between AIGN-owned methods and local adaptations



The AIGN Data Act Governance Framework 1.0

Derivative works or sector-specific adaptations may only be published with **written approval** from AIGN.

AIGN reserves the right to **audit, revoke, or publicly list** misuse or unauthorized certification activities.

Attribution Requirements

Wherever the AIGN Framework is referenced, used, or cited (in documents, tools, training, or platforms), the following **attribution statement** must be clearly visible:

“This structure is based on the AIGN Framework for Responsible AI Governance, developed by AIGN – Artificial Intelligence Governance Network (www.aign.global). All rights reserved.”

Misattribution or rebranding constitutes a violation of usage conditions and may result in legal recourse.

Certified Partnership and Licensing

Organizations wishing to:

- Offer AIGN-based **training**
- Perform **Trust Scan** or **Readiness Check** evaluations
- Issue or apply for **Trust Labels**
- Integrate AIGN tools into **commercial offerings**

...must apply for **AIGN Certified Partner Status**.

Criteria include:

- Signing a Partner Agreement
- Completing required training and tool onboarding
- Upholding AIGN values, reporting duties, and data handling standards
- Annual review and renewal (optional public listing on www.aign.global/partners)

How to Become a Partner:

Step 1: Apply via the AIGN website; Step 2: Complete required training; Step 3: Undergo a readiness review; Step 4: Sign partnership agreement and receive certification.



The AIGN Data Act Governance Framework 1.0

For any questions or to report suspected misuse of the framework, contact message@aign.global for clarification and next steps.

Enforcement and Jurisdiction

Any unauthorized use, reproduction, or misrepresentation of the AIGN Framework and its components may result in:

- Revocation of access or partnership
- Legal action under applicable intellectual property law
- Public delisting or warning

All legal disputes related to AIGN intellectual property or licensing shall be governed by the laws of the **Federal Republic of Germany**, with **Munich** as the agreed place of jurisdiction.

Closing Statement

The AIGN Framework was developed to serve the global public interest — but trust must be protected, and responsibility must be governed.

Open access does not mean ungoverned use.

By defining these terms, AIGN ensures that its mission can scale **without compromise, misuse, or dilution**.

If trust is the product — integrity is the process.

© 2025 AIGN – Artificial Intelligence Governance Network. All rights reserved.

This document and its contents are protected by international copyright and intellectual property laws. The AIGN Framework, its tools (including the Trust Scan, Global Trust Label, Education Trust Label, AI Readiness Check, and Agentic Risk Framework), visual elements, assessment logic, and all derived works are proprietary to AIGN unless otherwise noted.

No part of this document may be reproduced, distributed, translated, modified, reverse-engineered, or used in any commercial context without prior written permission from AIGN.



The AIGN Data Act Governance Framework 1.0

All trademarks and names mentioned herein are the property of their respective owners. References to third-party frameworks (e.g. EU AI Act, ISO/IEC 42001, NIST AI RMF, OECD AI Principles) are made for comparative and educational purposes only and imply no affiliation or endorsement.

This document is for informational and strategic use only and does not constitute legal advice, regulatory certification, or an audit instrument. AIGN accepts no liability for decisions made based on the use of this framework without proper implementation and contextual assessment.

27. Appendix: Glossary & Definitions

Management Summary

A unified language is essential for effective governance, compliance, and collaboration in the age of integrated Data & AI regulation. This glossary provides authoritative definitions for all core concepts used in the AIGN EU Data Act AI Governance Framework—ensuring clarity, traceability, and global usability for all users, auditors, and stakeholders.

Key Terms & Definitions

Data Intermediary

A neutral, regulated entity (as defined by the EU Data Governance Act, DGA) that facilitates secure, transparent, and non-discriminatory data sharing between data holders and data users, without using the data for its own purposes. Data intermediaries are subject to registration, oversight, and certification.

Data Trustee

A specialized form of data intermediary tasked with managing and protecting data on behalf of data subjects or data providers. Trustees act with fiduciary duty, ensuring rights, consent, and lawful data use at all times.

Data Altruism

The voluntary sharing of data by individuals or organizations for purposes of general interest—such as scientific research, public health, or social innovation—without seeking direct commercial benefit. Data altruism organizations must be registered and comply with transparency and consent rules set out in the DGA.

Trust Label (AIGN Trust Label)

A digital badge or certificate awarded to organizations that demonstrate full compliance with



The AIGN Data Act Governance Framework 1.0

the AIGN Framework—including the EU Data Act, AI Act, and DGA—across all relevant domains. The Trust Label serves as a public signal of operational trustworthiness and readiness for audit or procurement.

Maturity Level / Maturity Model

A structured, tiered system for evaluating and certifying the progress of an organization's Data & AI governance capabilities. Levels typically range from Initial (ad hoc, minimal controls) to By Design (fully embedded, continuous improvement). Each level is defined by specific requirements for roles, processes, documentation, and auditability.

Continuous Improvement

A governance principle and operational cycle in which organizations systematically review, update, and enhance their compliance, risk management, and governance processes—driven by incident learning, peer benchmarking, and regulatory changes.

Incident Sharing / Peer Learning

Structured, often anonymized exchange of real-world compliance, risk, or governance cases across organizations, aimed at accelerating learning, preventing repeat failures, and supporting sector-wide improvement.

Technical Interoperability

The ability of different data systems, platforms, or organizations to exchange, interpret, and use data seamlessly, based on open standards, machine-readable formats, and documented APIs. Interoperability is mandated by the EU Data Act and DGA for data portability and secure data sharing.

Data Access & User Rights Management

The operationalization of user, partner, and authority rights to access, export, delete, or manage data—ensuring compliance with the Data Act, GDPR, and sectoral laws. Includes audit trails, consent workflows, and user dashboards.

Contractual Fairness

A set of legal and operational principles ensuring that all contracts and data sharing agreements are fair, transparent, and non-discriminatory—covering access, rights, portability, dispute resolution, and exit conditions as required by the Data Act.

Certification / Certification Logic

The process, tools, and criteria by which an organization's compliance, maturity, and trustworthiness are assessed and attested (by self-assessment or third-party audit), leading to formal recognition (e.g. AIGN Trust Label, sectoral endorsements).

Audit Trail

A systematic, tamper-proof record of all relevant data, AI, or governance activities—such as



The AIGN Data Act Governance Framework 1.0

access, changes, sharing events, and incidents. Audit trails are essential for legal defense, certification, and regulatory review.

Data Provenance / Lineage

Documentation and evidence of the origin, transformation, and usage of data throughout its lifecycle. Required by the Data Act and AI Act for transparency, risk management, and compliance.

Stakeholder Engagement

Ongoing, structured involvement of all relevant parties—users, customers, partners, regulators, and the public—in governance, decision-making, and feedback processes. Promotes transparency, accountability, and legitimacy.

Data Room / Secure Processing Environment

A technical environment (virtual or physical) that enables controlled, auditable access and processing of sensitive or regulated data—meeting security, privacy, and compliance requirements (as per DGA and Data Act).