Journal of Decision Systems

ISSN: 1246-0125 (Print) 2116-7052 (Online) Journal homepage: www.tandfonline.com/journals/tjds20

From policy to action: a cross-regulatory conceptual framework to address data and AI regulations

Fangzhou Yu, Fergal Carton & Huanhuan Xiong

To cite this article: Fangzhou Yu, Fergal Carton & Huanhuan Xiong (2026) From policy to action: a cross-regulatory conceptual framework to address data and AI regulations, Journal of Decision Systems, 35:1, 2669329, DOI: 10.1080/12460125.2026.2669329

To link to this article: https://doi.org/10.1080/12460125.2026.2669329

Published online: 17 May 2026.

JOURNAL OF DECISION SYSTEMS
2026, VOL. 35, NO. 1, 2669329
https://doi.org/10.1080/12460125.2026.2669329

From policy to action: a cross-regulatory conceptual framework to address data and AI regulations

Fangzhou Yu, Fergal Carton and Huanhuan Xiong

Cork University Business School, University College of Cork, Cork, Ireland

ABSTRACT

Organisations operating in data- and AI-intensive environments face an increasingly fragmented and overlapping EU regulatory landscape, including the GDPR, AI Act, etc. Existing research largely addresses these regimes in isolation, offering limited guidance on integrated organisational compliance. This study develops a cross-regulatory integration framework that translates multi-regulatory obligations into structured organisational capabilities, explicitly assigning clear actors and responsibilities. Drawing on Actor-Network Theory (ANT) and a Strategic-Tactical-Operational (STO) decision-layer model, this study conceptualises compliance as a networked and multi-level governance process. The framework supports organisations in aligning ethical criteria, technical controls, and governance responsibilities across regulatory domains, advancing enterprise-wide digital governance and compliance management through both operational and functional processes.

ARTICLE HISTORY
Received 18 February 2026
Accepted 24 April 2026

KEYWORDS
GDPR; AI ACT; cross-regulatory compliance; Actor-Network Theory

1. Introduction

Organisations operating in contemporary digital environments increasingly rely on data and advanced technologies, particularly artificial intelligence (AI), to enhance efficiency, innovation, and value creation (Wamba-Taguimdje et al., 2020). At the same time, these activities are subject to expanding regulatory constraints that require organisations to balance technological benefits with legal, ethical, and societal obligations. Within the European Union (EU), this regulatory landscape has evolved rapidly. The General Data Protection Regulation (GDPR), enacted in 2016, harmonises data protection rules across Member States and strengthens individuals' control over personal data. The proposed EU AI Act introduces a risk-based framework for governing AI systems and their deployment. Beyond these horizontal instruments, organisations must also comply with cross-cutting and sector-specific regulations, including the Digital Services Act (DSA) governing digital services, the NIS2 Directive addressing cybersecurity and network resilience, the Digital Markets Act (DMA) regulating digital markets, as well as sector-specific healthcare instruments such as the European Health Data Space (EHDS) and the Medical Device Regulation (MDR).

Organisations operating in data- and AI-intensive environments must therefore systematically interpret overlapping regulations and translate them into concrete compliance actions through structured implementation, coordination, and training. However, the proliferation of interdependent regulations creates a complex, multi-layered compliance environment that organisations struggle to absorb and operationalise coherently (Jørgensen & Ma, 2025). Existing literature largely examines individual regulations in isolation and offers limited organisational guidance on managing compliance across multiple regulatory regimes. Moreover, the distribution of responsibility between legal norms and organisational actors remains insufficiently theorised (Labadie & Legner, 2023; Schmidt et al. 2024; Tikanmäki et al., 2025). To address these gaps, this paper develops a cross-regulatory framework that supports organisations in translating regulatory requirements into practical compliance tasks and organisational capabilities. Drawing on Actor-Network Theory (ANT), the study conceptualises digital regulation as a network of heterogeneous actors and combined with a three-layer organisational decision-making model: strategic, tactical, and operational (STO), to allocate compliance tasks and responsibilities to appropriate organisational levels. This paper

CONTACT Fangzhou Yu fangzhou.yu@umail.ucc.ie Cork University Business School, O'Rahilly Building (Block B, Room 2.37/2.38), College Road, University College of Cork, Cork, Ireland (T12 K8AF)

makes two primary contributions. First, it advances the literature by proposing a conceptual framework that structures organisational compliance across data and AI regulations. Second, it responds to calls for a reconceptualisation of enterprise-wide digital governance (Jakobi et al., 2020; Labadie & Legner, 2023) by clarifying responsibility distribution and operationalising ethical and regulatory criteria in organisational practice.

The remainder of the paper is structured as follows. Section 2 reviews the relevant literature on GDPR and AI Act compliance. A conceptual framework for cross-regulatory capabilities is then presented in Section 3, together with a summary of the core ethical criteria. Section 4 develops the STO model as an organisational implementation logic, and the paper concludes in Section 5 with limitations and implications.

2. Literature review and theoretical background

2.1. Data and AI governance literature state

Research on 'GDPR compliance' and 'AI Act compliance' increasingly conceptualises regulatory obligations through the lenses of data governance and AI governance. Data governance scholarship focuses on data collection (Labadie & Legner, 2023), consent (Politou et al., 2018), privacy (Mestari et al., 2023), data protection (Murdoch, 2021), and data ownership and sharing (Kranz et al., 2023; Trier et al., 2022), whereas AI governance centres on algorithmic transparency (Bitzer et al., 2023), fairness (Greene et al., 2023), and explainability (Bork et al., 2023), highlighting the difficulty of rendering AI-driven decisions accountable to affected stakeholders (Horneber & Laumer, 2023; Trier et al., 2022). Across both domains, personal and sensitive data (e.g. health, financial, and behavioural data) constitute the primary risk locus, as their reuse across organisational and technical contexts generates compounded privacy, security, and ethical risks throughout the data and AI lifecycle (Janssen et al., 2020; Mestari et al., 2023). Empirical evidence links governance weaknesses to increased cyber risk and data breaches (Murdoch, 2021), while machine-learning systems introduce bias and discrimination risks affecting vulnerable populations (Mitchell et al., 2021; Obermeyer et al., 2019). GDPR Enforcement case analyses further identify recurring technological risk categories, including insufficient safeguards, video surveillance and automated decision-making and profiling (Akhlaghpour et al., 2021), indicating that regulatory attention converges on strengthening technical safeguards (e.g. pseudonymisation, encryption, and strict access controls) (Asghar et al., 2019) and ensuring human oversight across the system lifecycle (Almagrabi & Khan, 2025).

At the organisational level, compliance is increasingly framed as a multi-stakeholder process extending beyond legal functions to technical and operational actors (Jakobi et al., 2020; Labadie & Legner, 2023). Recent frameworks attempt to structure this complexity: Schmidt and Wilhelm (2000) conceptualise AI regulatory governance across dimensions, including data processing, technology assessment, innovation support, and human rights, while Tikanmäki et al. (2025) operationalise compliance through structured categories covering AI systems, data operations, risk assessment, transparency, accountability, and lifecycle management. These frameworks provide structuring logics for understanding the scope of compliance. However, they remain conceptual and fragmented, often separating data, AI, and risk without clearly linking them to concrete regulatory obligations. It remains unclear how organisations can translate overlapping legal requirements into coherent, operational governance practices, which constitutes the gap addressed in this study.

2.2. Actor-Network Theory

Actor-Network Theory, originating from science and technology studies, provides a relational and process-oriented approach for analysing how social order, technologies, and organisational practices are produced through networks of heterogeneous actors (Durepos, 2008). Within the broader body of organisational and governance theories, several alternative perspectives offer relevant but partial explanations. For instance, Stakeholder Theory (Phillips et al., 2003) focuses primarily on human actors and their interests, and Sociotechnical Systems Theory (Appelbaum, 1997) emphasises the interplay between social and technical elements but often treats technology as context rather than active participant, ANT uniquely conceptualises both human and non-human entities, such as regulators, managers, AI systems, datasets, policies, standards,

and documentation, as 'actors' (or actants) that actively participate in shaping outcomes. This study draws on ANT to conceptualise digital compliance not as a fixed legal process, but as a dynamic real-time network in which regulatory texts (e.g. GDPR), organisational roles, technical artefacts, and operational practices mutually shape and stabilise one another. In a typical scenario involving AI systems within organisations, duties are typically allocated to the model provider, model hoster, and model integrator, each bearing distinct compliance and security obligations shaped by contractual arrangements and degrees of technical control (Bunzel, 2025). Applying ANT enables the systematic identification of key compliance actors, including legally defined roles (e.g. controllers, processors), organisational units, technical infrastructures, risk assessment tools, logs, and reporting mechanisms, and facilitates analysis of how responsibilities are distributed, translated, or fragmented across the compliance lifecycle. These insights inform the design of the cross-regulatory framework in this study and are operationalised in the multi-layer model presented in Section 4.

2.3. STO decision layers as an organisational implementation logic

Beyond ANT's analytical capacity to identify heterogeneous actors and their interactions, this study adopts the Strategic-Tactical-Operational decision-layer model (Ballou, 1973) as an organisational implementation logic to guide the practical structuring of compliance activities. The STO framework distinguishes three interdependent levels of decision-making: strategic decisions that establish long-term direction and governance priorities; tactical decisions that translate strategic intent into plans, standards, and coordination mechanisms; and operational decisions that govern day-to-day execution and system use. Its core strength lies in separating concerns while preserving alignment: strategic decisions define 'what' and 'why', tactical decisions determine 'how' and 'by whom', and operational decisions enact compliance in practice. In multi-regulatory contexts, this layered structure effectively enables continuous interpretation, operationalisation, and monitoring of abstract legal obligations across organisations.

3. Digital regulations and ethical capability

This section introduces the EU regulatory framework and synthesises academic insights on compliance capabilities, design principles, and recurring challenges. To achieve regulatory compliance, organisations are advised to navigate requirements originating from three distinct but interdependent regulatory domains: data regulation, technology regulation, and sector-specific regulation, as shown in Figure 1. Each domain introduces its own principles, obligations, and compliance challenges. At the intersection of these three domains lies the central objective of this study: to develop cross-regulatory compliance guidance that integrates regulatory principles into coherent organisational capabilities.

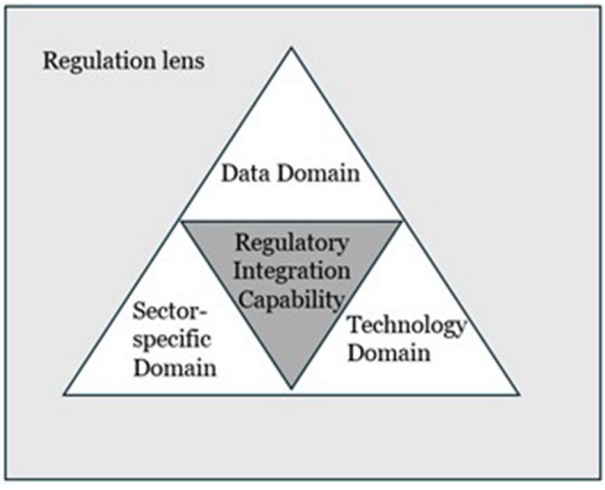

Figure 1. A conceptual framework for cross-regulatory integration capability in organisational compliance.

3.1. Data lens – GDPR

GDPR establishes foundational principles governing the processing of personal data in the EU. GDPR mandates explicit, informed, and revocable user consent, requiring organisations to clearly articulate the purpose of data collection and to provide mechanisms that allow data subjects to withdraw consent at any time. The regulation further enshrines the principle of data minimisation, stipulating that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed, thereby embedding privacy-by-design into organisational systems. Additionally, the right to be forgotten grants individuals the right to request the erasure of their personal data under specific conditions, such as when the data is no longer necessary or when consent has been withdrawn, reinforcing user control over digital identities. GDPR adopts a risk-based regulatory approach, granting organisations a degree of discretion in how compliance measures are implemented, while still holding them accountable for outcomes (Akhlaghpour et al., 2021).

3.2. Technology lens – AI ACT

Building on the data protection regime, the EU AI Act represents the first horizontal regulatory framework governing AI technologies. It introduces a risk-based classification system that distinguishes between unacceptable, high-risk, limited-risk, and minimal-risk AI applications, each subject to differentiated obligations (European Commission, 2021). Academic studies emphasise governance capabilities related to risk assessment, human oversight, transparency, documentation, and lifecycle monitoring as central to AI Act compliance. At the same time, scholars note that certain sector-specific risks, such as AI-enabled market manipulation and cybersecurity threats, remain only partially addressed, creating ongoing compliance uncertainty (Niet et al., 2021).

3.3. Sector-specific lens

Beyond horizontal regulations such as the GDPR and the AI Act, organisations must also comply with sector-specific regulatory regimes that significantly intensify compliance complexity. Evidence from GDPR enforcement illustrates this shift. By 2025, the Irish Data Protection Commission (DPC) had issued cumulative fines totalling approximately €3.5 billion (Data Protection Commission, 2025). Although this figure represents a decline from earlier peak years, the number of fines imposed on organisations in the finance, energy, and healthcare sectors continues to increase. These enforcement patterns highlight that compliance challenges are not uniform across industries. Instead, sector-specific operational contexts, data types, and risk profiles shape how regulatory requirements are interpreted and enforced. In healthcare, regulatory compliance is particularly demanding due to the sensitivity of patient data and the direct implications for fundamental rights and safety. These sectoral differences are further reinforced by overlapping regulatory regimes (e.g. EHDS and MDR in healthcare; DMA in digital markets), which impose heightened and interdependent obligations on data governance, AI oversight, cybersecurity, and operational resilience, thereby requiring organisations to move beyond fragmented compliance mechanisms towards integrated cross-regulatory governance.

3.4. Ethical criteria for cross-regulatory compliance

Through a structured interpretive approach informed by an analytical framework of EU digital regulation, a cross-regulatory comparison was conducted to identify the intersection of recurring normative requirements across the selected instruments. This process resulted in the eleven ethical criteria presented in Table 1. Only those principles that consistently appear and are operationalised in multiple regulations were retained, thereby reflecting the overlapping ethical foundations underlying GDPR, AI Act, and sector-specific regimes. This mapping adopts a functional rather than a purely doctrinal perspective. Legal texts are interpreted according to the primary ethical objective they serve, which may not always align with their formal legal classification. Consequently, the framework is intended as a conceptual synthesis tool rather than a comprehensive legal interpretation. Its purpose is to make visible the shared ethical structure beneath

Table 1. Core ethical criteria for data & AI governance.

	Regulations						
	Data	Technique			Sector-specific		
Criteria	GDPR	AI Act	DSA	NIS2	DMA	EHDS	MDR
(a) Transparency	Art. 5(1)(a), 12–14	Art. 13, 52	Art. 14, 15, 24	Art. 21(2)(d)	Art. 6, 13	Art. 3–5	Art. 10, 27
(b) Justice and fairness	Art. 5(1)(a), 22	Art. 10(2), 71	Art. 14		Art. 6		
(c) Responsibility	Art. 5(2), 24	Art. 16, 17	Art. 4	Art. 20	Art. 8		Art. 10
(d) Privacy	Art. 6, 9, 25	Art. 10				Art. 33	
(e) Non-maleficence	Art. 32	Art. 9	Art. 34	Art. 21			Art. 10
(f) Integrity	Art. 5(1)(f)	Art. 15		Art. 21(2)(b)			Art. 10
(g) Traceability	Art. 30	Art. 12, 18	Art. 24	Art. 23			Art. 25
(h) Education & Training	Art. 39(1)(b)	Art. 14(4)		Art. 21(2)(g)		Art. 11	Art. 10
(i) Security (cybersecurity, confidentiality)	Art. 32	Art. 15	Art. 32	Art. 21		Art. 37	Art. 17
(j) Risk Management	Art. 24, 35	Art. 9	Art. 34, 35	Art. 21	Art. 34		Art. 10
(k) Monitoring & Reporting	Art. 33, 34	Art. 61, 62	Art. 15, 42	Art. 23	Art. 11		Art. 87

regulatory requirements, while acknowledging that compliance in practice arises from overlapping and mutually reinforcing obligations rather than isolated adherence to individual articles or criteria. These eleven ethical criteria will assist in aligning regulatory principles with organisational practice, and a multi-level actor-network governance framework to operationalise this alignment will be advanced in the next section.

4. Multi-level actor-network governance

Prior literature and official guidance have identified compliance tasks, but they remain limited in explaining how these tasks should be translated into concrete actions and aligned with organisational roles. This section addresses the gap by consolidating governance tasks from the literature and translating them into role-specific, actionable responsibilities. The STO model is applied vertically to establish a hierarchical decision-making architecture, providing a multi-layered organisational structure that reflects a top-down, temporally ordered decision logic from governance intent to execution. Complementing this vertical structure, ANT is employed horizontally within each layer to support the identification of governance actions and their allocation to the appropriate actor. By integrating STO's layered hierarchy with ANT's relational dynamics, the framework reorganises the conceptual dimensions into a coherent pyramid structure (Figure 2). In this structure, technology, data, and sector-specific requirements presented in Figure 1 constitute the surface dimensions. Within the pyramid, compliance activities are distributed across strategic, tactical, and operational implementation layers, each corresponding to different levels of decision-making and execution while simultaneously addressing all three regulatory domains. The framework integrates complementary governance mechanisms, including structural mechanisms (e.g. formal roles, policies, committees), procedural

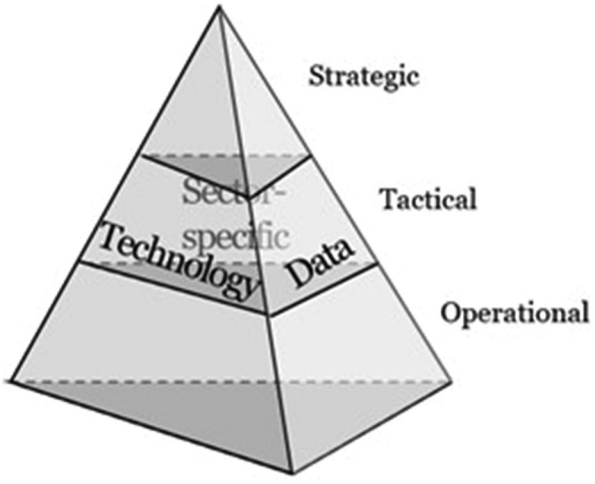

Figure 2. A multi-level organisational governance theoretical framework integrating actor-network Theory and STO layers.

mechanisms (e.g. standards, training programmes, assessments), and relational mechanisms (e.g. cross-functional coordination and communication). For each layer, specific actors are linked to defined governance actions. The description of these actions draws on enterprise-oriented compliance guidance, including but not limited to the DPC GDPR Readiness Checklist (2026) and the AI Act Compliance Matrix (Fazlioglu, 2024), which are elaborated in the following subsections.

4.1. Strategic layer: vision, accountability, and governance design

The letters in parentheses (a, c, h, etc.) refer to the core ethical and compliance criteria listed in Table 1

The strategic layer, located at the top of the governance pyramid, addresses long-term and high-impact decisions that shape an organisation's overall direction, risk appetite, and compliance posture. Strategic choices include defining acceptable AI use cases, allocating accountability roles, and making architectural decisions like data separation or modular system design to limit regulatory exposure (Fast et al., 2023). This layer is also responsible for resource allocation and approval. Legal compliance costs, technical upgrades, and administrative burdens compete with innovation and operational growth. Under the GDPR, strategic decisions include defining the purposes and boundaries of data processing, establishing escalation and reporting lines, and formalising legally required roles such as Data Protection Officers (DPOs), Chief Data Officers (CDOs), Chief AI Officers (CAIO), and data controllers and processors. Organisations are also required to ensure structured cooperation with supervisory authorities. Similarly, the EU AI Act requires organisations to articulate intended AI use cases, align AI deployment with organisational values and sectoral objectives, and assign governance responsibility for high-risk AI systems. Recent literature further proposes the appointment of roles such as a Complaint Oversight Officer to oversee complaint-handling and stakeholder challenge mechanisms (Hollanek et al., 2025).

4.2. Tactical layer: translation, coordination, and planning

The tactical layer bridges strategic intent and operational execution by converting high-level regulatory objectives into medium-term plans, standards, and coordination mechanisms, with a focus on implementing compliance across organisational units, projects, and functions.

In the GDPR context, tactical activities include designing data lifecycle management standards, conducting Data Protection Impact Assessments (DPIAs), and operationalising principles such as purpose limitation and data minimisation. Under the AI Act, tactical compliance involves classifying AI systems by risk category, defining documentation requirements, and planning human oversight and risk management measures for high-risk applications. 'Networks' are particularly important at the tactical layer, where compliance relies on effective coordination among legal, technical, and business teams across departments and external actors. This involves negotiating shared standards, responsibility transfers, and implementation boundaries. Organisations increasingly rely on interdisciplinary teams to bridge the 'translation gap' between abstract legal requirements and concrete technical specifications (Jørgensen & Ma, 2025). Cross-functional training, shared vocabularies, and structured collaboration processes are critical to bridging the translation gap between abstract legal requirements and concrete technical specifications. This layer also drives the design of internal guidelines, toolkits, and workflows aligned with value and holistic expertise (Hollanek et al., 2025).

4.3. Operational layer: execution, monitoring, and iteration

The operational layer forms the base of the pyramid in Figure 2 and focuses on day-to-day compliance execution by frontline actors, including not only technical staff such as data engineers and IT teams, but also nearly all employees across the organisation. Operational responsibilities encompass participation in compliance and ethics training, maintaining operational records, and reporting incidents such as data breaches, cybersecurity risks, or AI bias. Effective operational governance also relies on upward feedback loops, whereby monitoring outcomes and incidents informs tactical adjustments and, where necessary, prompts strategic reconsideration of governance structures or AI deployment choices.

In the AI context, explainable AI (XAI) research seeks to ensure that decision-makers can understand and trust system outputs during use. However, many current XAI techniques generate only post-hoc

explanations without modifying the underlying model (Bork et al., 2023). Moreover, there exists a fundamental trade-off between model performance and explainability, and generating faithful, contestable explanations at scale is often computationally expensive (Adadi & Berrada, 2018).

4.4. Practical implementation: compliance tasks map

The task identifiers correspond to the coded actions presented in Tables 2–4.

To translate the multilevel actor-network governance framework from high-level policy into repeatable organisational actions, this subsection introduces compliance tasks and roles allocation map (Figure 3). Structured as an ITIL 4 service value stream (Axelos, 2019), this map serves as a practical tool for orchestrating governance activities across multiple actors and stakeholders. The framework is organised into five sequential stages, mirroring the ITIL Service Value Chain (SVC) to ensure logical execution: The Planning and Design (Plan & Design, ITIL-SVC) stage establishes the normative and strategic foundation by aligning regulatory interpretation with organisational values and formalising policies that define the direction of compliance. Building on this, the Deployment (Obtain/Build & Transition, ITIL-SVC) stage translates these principles into actionable organisational arrangements by embedding responsibilities, allocating resources, and configuring processes, safeguards, and accountability structures. The Operation (Deliver & Support, ITIL-SVC) stage then realises compliance in practice, where regulatory requirements are enacted through everyday activities such as secure data handling, AI system operation, human oversight, and staff training. To ensure consistent implementation, the Monitoring (Improve, ITIL-SVC) stage introduces systematic oversight through evaluation, record-keeping, and incident reporting, enabling continuous refinement of

Table 2. Strategic-layer actor-Action mapping for multi-regulatory compliance.

ANT Roles Human	Non-human	Action (Translation in practice)
Executive	Ethical literacy goals (strategy/policies), resources(budgets/tools)	[1] Establish ethical literacy goals (a, c, h); [2] Allocate positions (c, h); [3] Allocate resources (c, h, i)
DPO	Compliance policies, accountability frameworks	[4] Endorse policies (c, h); [5] Define the compliance strategy (c, j); [6] Set accountability structures (c); [7] Cooperate, communicate, and report to external review authorities (DPC) (c, k)
Legal	Regulations (legal texts)	[8] Interpret regulations (a, b, c, d); [9] Manage liability and external accountability relations (c)
Third-party	Datasets, models	[10] Clarification of party-specific data or AI lifecycle processes (f, g); [11] Co-negotiated data transfer standard and safeguards (f, g, i)

Table 3. Tactical-layer actor-Action mapping for multi-regulatory compliance.

ANT Roles Human	Non-human	Action (Translation in practice)
DPO	Processing records; automatic record tools	[12] Monitor daily processes (k); [13] Vet records (k); [14] Evaluate processes (k); [15] Set incident response plan (i, j, k); [16] Gather feedback and drive improvement (k)
Data engineers	Dataset, models	[17] Formulate secure data pipelines (f, i); [18] Set internal and external data transfer standards (f, i)
IT	Dataset; AI System	[19] Conduct AI system impact and risk assessment (j)
HR	Training materials/ platforms	[20] Provide staff training on compliance processes (h)

Table 4. Operational-layer actor-Action mapping for multi-regulatory compliance.

ANT Roles Human	Non-human	Action (Translation in practice)
IT	Automatic record tools; User consent	[21] Ensure AI transparency and explainability (a); [22] Support customer consent drafting (d); [23] Human intervention on automatic processing system (b, c); [24] System monitoring and recording (k)
Data manager	Data encryption technology; User consent; Dataset	[25] Support customer consent drafting (d); [26] Manage user consent (d); [27] Implement data encryption (anonymisation/pseudonymisation) (d, f, i); [28] Format data to standards (f); [29] Ensure secure data pipelines (f, i)
All staff	Processing records	[30] Profile data and technique processes (k); [31] Report incidents (k)

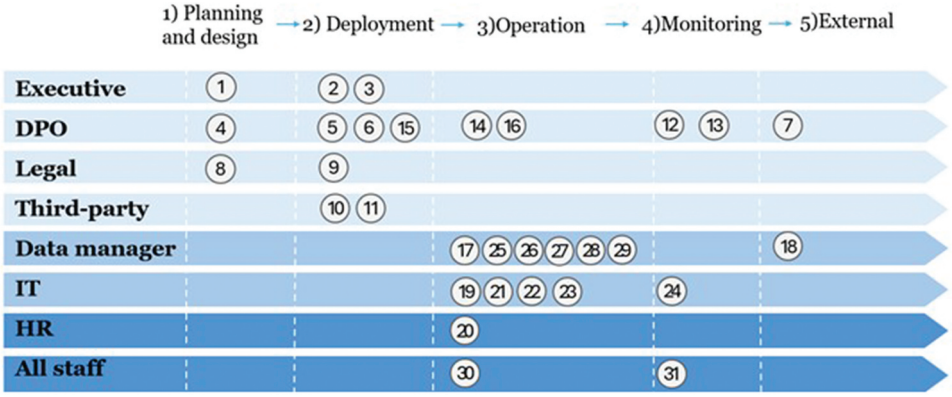

Figure 3. Compliance tasks roles allocation Map.

processes. Finally, the External (Engage, ITIL-SVC) stage extends governance beyond organisational boundaries by coordinating with regulators and external stakeholders, ensuring alignment with evolving regulatory expectations and accountability requirements. Building on the actor-action mapping in previous subsections, this map clearly allocates each task to relevant specialist roles, indicates the necessary prerequisites between tasks, and thereby reduces ambiguity, minimises responsibility gaps, and enables teams to execute compliance activities systematically in everyday organisational practice.

5. Conclusion and outlook

This study aims to support organisations in finding a balance between regulatory compliance and innovation, enabling value creation in AI-driven markets while maintaining accountability and trust (Pfeiffer et al., 2024). Drawing on an extensive review of the literature, it examines organisational compliance capabilities and develops a multi-dimensional, regulation-oriented conceptual framework. The study combines Actor-Network Theory with the Strategic-Tactical-Operational decision model and proposes a three-layer governance framework, together with a practical action workflow map. For researchers, the framework offers a conceptual foundation for future empirical investigation of organisational governance practices and compliance artefact design. For practitioners, it provides clear logic for role and responsibility allocation across the data and AI lifecycle, supporting legally and ethically grounded decision-making and implementation. While the model is designed to be generalisable, its regulatory focus is on the EU landscape. Nevertheless, it allows for contextual adaptation in real-world scenarios, enabling organisations to adjust role configurations according to managerial and financial resources, sectoral conditions, and local regulations.

Acknowledgments

The data used in this study are publicly available. Processed data supporting the findings are available from the author upon reasonable request.

Author contributions

CRediT: **Fangzhou Yu:** Data curation, Resources, Writing – original draft; **Fergal Carton:** Formal analysis, Methodology, Supervision, Validation, Visualization, Writing – review & editing; **Huanhuan Xiong:** Formal analysis, Investigation, Methodology, Supervision, Validation, Visualization, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Fangzhou Yu http://orcid.org/0009-0003-8846-8360

References

Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access*, *6*, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052

Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A., & Hynd, A. (2021). Learning from enforcement cases to manage GDPR risks. *MIS Quarterly Executive*, 199–218. https://doi.org/10.17705/2msqe.00049

Almagrabi, A., & Khan, R. (2025). Optimizing secure AI lifecycle model management with innovative generative AI strategies. *IEEE Access*, *13*, 12889–12920. https://doi.org/10.1109/access.2024.3491373

Appelbaum, S.H. (1997). Socio-technical systems theory: An intervention strategy for organizational development. *Management Decision*, *35*(6), 452–463. https://doi.org/10.1108/00251749710173823

Asghar, M., Kanwal, N., Lee, B., Fleury, M., Herbst, M., & Qiao, Y. (2019). Visual surveillance within the EU General Data Protection Regulation: A technology perspective. *IEEE Access*, *7*, 111709–111726. https://doi.org/10.1109/access.2019.2934226

Axelos, L. (2019). *Itil® 4 foundation revision guide*. The Stationery Office Ltd.

Ballou, R.H. (1973). *Business logistics management*. Prentice-Hall.

Bitzer, T., Wiener, M., & Cram, W.A. (2023). Algorithmic transparency: Concepts, antecedents, and consequences-a review and research framework. *Communications of the Association for Information Systems*, *52*(1), 293–331. https://doi.org/10.17705/1CAIS.05214

Bork, D., Ali, S.J., & Dinev, G.M. (2023). AI-enhanced hybrid decision management. *Business & Information Systems Engineering*, *65*(2), 179–199. https://doi.org/10.1007/s12599-023-00790-2

Bunzel, N. (2025). Compliance made practical: Translating the EU AI Act into implementable security actions. In *2025 IEEE/ACM International Workshop on Responsible AI Engineering (RAIE)* 2025 (IEEE) (pp. 69–73). https://ieeexplore.ieee.org/abstract/document/11029418/citations#citations

Data Protection Commission. (2025). Data Protection Commission 2024 annual report. https://www.dataprotection.ie/en/data-protection-commission-publishes-2024-annual-report

Data Protection Commission. (2026). GDPR readiness self-assessment checklist. https://dataprotection.ie/en/organisations/resources-organisations/self-assessment-checklist

Durepos, G. (2008). Reassembling the social: An introduction to actor-network-theory. *Equality, Diversity and Inclusion*, *27*(3), 307–309. https://doi.org/10.1108/eoi.2008.27.3.307.2

European Commission. (2021). Proposal for a regulation laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. *Frontiers in Artificial Intelligence*, *4*, 690237. https://doi.org/10.3389/frai.2021.690237

Fast, V., Schnurr, D., & Wohlfarth, M. (2023). Regulation of data-driven market power in the digital economy: Business value creation and competitive advantages from big data. *Journal of Information Technology*, *38*(2), 202–229. https://doi.org/10.1177/02683962221114394

Fazlioglu, M. (2024). Eu AI Act compliance matrix. IAPP. https://iapp.org/resources/article/eu-ai-act-compliance-matrix

Greene, T., Shmueli, G., & Ray, S. (2023). Taking the person seriously: Ethically aware is research in the era of reinforcement learning-based personalization. *Journal of the Association for Information Systems*, *24*(6), 1527–1561. https://doi.org/10.17705/1jais.00800

Hollanek, T., Pi, Y., Peters, D., Yakar, S., & Drage, E. (2025). The EU AI Act in development practice: A pro-justice approach. arXiv preprint arXiv: 2504.20075.https://doi.org/10.48550/arXiv.2504.20075

Horneber, D., & Laumer, S. (2023). Algorithmic accountability. *Business & Information Systems Engineering*, *65*(6), 723–730. https://doi.org/10.1007/s12599-023-00817-8

Jakobi, T., von Grafenstein, M., Legner, C., Labadie, C., Mertens, P., Öksüz, A., & Stevens, G. (2020). The role of is in the conflicting interests regarding GDPR. *Business & Information Systems Engineering*, *62*(3), 261–272. https://doi.org/10.1007/s12599-020-00633-4

Janssen, M., Brous, P., Estevez, E., Barbosa, L.S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly*, *37*(3), 101493. https://doi.org/10.1016/j.giq.2020.101493

Jørgensen, B.N., & Ma, Z.G. (2025). Regulating AI in the energy sector: A scoping review of EU laws, challenges, and global perspectives. *Energies*, *18*(9), 2359. https://doi.org/10.3390/en18092359

Kranz, J., Kuebler-Wachendorff, S., Syrmoudis, E., Grossklags, J., Mager, S., Luzsa, R., & Mayr, S. (2023). Data portability. *Business & Information Systems Engineering*, *65*(5), 597–607. https://doi.org/10.1007/s12599-023-00815-w

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16–44. https://doi.org/10.1177/02683962221141456

Mestari, S., Lenzini, G., & Demirci, H. (2023). Preserving data privacy in machine learning systems. *Computers & Security*, *137*, 103605. https://doi.org/10.1016/j.cose.2023.103605

Mitchell, S., Potash, E., Barocas, S., D'Amour, A., & Lum, K. (2021). Algorithmic fairness: Choices, assumptions, and definitions. *Annual Review of Statistics and Its Application*, *8*(1), 141–163. https://doi.org/10.1146/annurev-statistics-042720-125902

Murdoch, B. (2021). Privacy and artificial intelligence: Challenges for protecting health information in a new era. *BMC Medical Ethics*, *22*(1), 122. https://doi.org/10.1186/s12910-021-00687-3

Niet, I., van Est, R., & Veraart, F. (2021). Governing AI in electricity systems: Reflections on the EU artificial intelligence bill. *Frontiers in Artificial Intelligence*, *4*, 690237. https://doi.org/10.3389/frai.2021.690237

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

Pfeiffer, J., Lachenmaier, J.F., Hinz, O., & van der Aalst, W. (2024). New laws and regulation. *Business & Information Systems Engineering*, *66*(6), 653–666. https://doi.org/10.1007/s12599-024-00902-6

Phillips, R., Freeman, R.E., & Wicks, A.C. (2003). What stakeholder theory is not. *Business Ethics Quarterly*, *13*(4), 479–502. https://doi.org/10.5840/beq200313434

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), tyy001. https://doi.org/10.1093/cybsec/tyy001

Schmidt, G., & Wilhelm, W. (2000). Strategic, tactical and operational decisions in multi-national logistics networks: A review and discussion of modelling issues. *International Journal of Production Research*, *38*(7), 1501–1523. https://doi.org/10.1080/002075400188690

Schmidt, J., Schutte, N.M., Buttigieg, S., Novillo-Ortiz, D., Sutherland, E., Anderson, M., de Witte, B., Peolsson, M., Unim, B., Pavlova, M., Stern, A.D., Mossialos, E., & van Kessel, R. (2024). Mapping the regulatory landscape for artificial intelligence in health within the European Union. *NPJ Digital Medicine*, *7*(1), 229. https://doi.org/10.1038/s41746-024-01221-6

Tikanmäki, I., Burns, F., Edelberg, J., Kuivanen, P., Tuomi, E., & Ylimaa, J. (2025). AI governance: Achieving EU AI Act compliance in the Dynamo project. *European Conference on Cyber Warfare and Security*, *24*(1), 875–878. https://doi.org/10.34190/eccws.24.1.3378

Trier, M., Kundisch, D., Beverungen, D., Müller, O., Schryen, G., & Mirbabaie, M. (2022). Digital responsibility. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4026082

Wamba-Taguimdje, S., Wamba, S., Kamdjoug, J., & Wanko, C. (2020). Influence of artificial intelligence (AI) on firm performance: The business value of AI-based transformation projects. *Business Process Management Journal*, *26*(7), 1893–1924. https://doi.org/10.1108/BPMJ-10-2019-0411