Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 09| 2025

Research Article **Received:** 20-07-2025| **Accepted:** 10-08-2025 | **Published:** 04-09-2025

Compliance-aware AI: Embedding Regulatory Logic into Machine Learning Pipelines

Heena Piratiyath

The University of Texas at Austin, Texas, USA

Abstract: This article addresses the emerging challenge of ensuring regulatory compliance in artificial intelligence systems. While traditional software relies on explicit rule-based logic to enforce compliance requirements, modern machine learning models operate on probabilistic foundations that introduce novel compliance risks. The article explores methodologies for embedding regulatory logic—including age verification, consent management, and access controls—directly into AI pipelines. Through an examination of pre-processing filters, post-processing safeguards, and runtime governance mechanisms, architectural patterns are presented that can help AI practitioners design systems that maintain compliance even when working with dynamic or black-box models. This framework offers practical guidance for AI product teams operating in highly regulated domains.

Keywords: Regulatory compliance, Machine learning governance, Compliance-by-design, AI transparency, Probabilistic decision-making.

INTRODUCTION

The rapid proliferation of artificial intelligence (AI) systems across industries has created a significant tension between innovation and regulatory compliance. While traditional software systems implement compliance through deterministic logic and explicit rule-based constraints, modern machine learning (ML) approaches operate on fundamentally different principles. The probabilistic nature of ML models, combined with their often opaque decision-making processes, introduces novel compliance challenges that traditional software engineering approaches fail to address adequately.

Regulatory frameworks worldwide—from GDPR in Europe to HIPAA in healthcare and financial regulations like Basel III—impose specific requirements on information systems, including those powered by AI. These frameworks create implementation challenges for organizations deploying machine learning systems in regulated environments, as documented in fairness and machine learning studies examining the limitations of technical solutions to regulatory problems (Hacker, P. *et al*., 2022). Existing compliance models often struggle with the inherent characteristics of ML systems, where decision boundaries are probabilistic rather than deterministic.

For AI product teams working in regulated environments, these requirements cannot be treated as afterthoughts. Compliance must be designed into the core architecture of machine learning pipelines from inception. The structured pipeline approach to ML development provides natural integration points for compliance mechanisms at each stage of the workflow (Google.com,). By organizing machine learning workflows into discrete stages—from data collection through deployment and monitoring—teams can implement appropriate controls at each point where compliance risks might emerge.

The integration of compliance considerations into machine learning pipelines requires methodological approaches that address both technical and organizational dimensions. Modern ML pipeline architectures provide mechanisms to enforce consistent data handling, feature transformation, model training constraints, and output validation (Google.com,). These architectures can be extended to incorporate regulatory logic directly into automated workflows, ensuring consistent application of compliance requirements.

This article explores methodological approaches to embedding regulatory logic directly into AI systems, focusing on architectural patterns that can be implemented across the ML lifecycle. It examines how compliance requirements can be translated into technical controls at each stage of an AI pipeline, from data collection and preprocessing to model training, deployment, and runtime monitoring. By implementing compliance controls at each pipeline stage, organizations can build systems that maintain regulatory alignment even when working with complex, dynamic, or black-box models.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

***Corresponding Author:** Heena Piratiyath

DOI- https://doi.org/10.5281/zenodo.17055703

THE COMPLIANCE GAP IN MODERN AI SYSTEMS

Traditional Software Compliance vs. AI Compliance

Conventional software infrastructures effectuate compliance through well-grounded patterns that have matured across decades of software engineering evolution. These methodological approaches encompass input verification procedures, role-oriented access management (RBAC), business directive engines, transaction documentation, and anomaly containment protocols. Such operational mechanisms depend upon deterministic logical constructs and unambiguous demarcations between system constituents. A financial services application, as an illustrative example, might implement a straightforward directive: "Should the user's chronological age register below 18 years, categorically reject the loan petition." These directives manifest explicitly, transparently, and with intrinsic auditability, thereby furnishing incontrovertible substantiation of compliance intentionality and practical enforcement (Kleinberg, J. *et al*., 2016).

Machine learning algorithmic frameworks, through contrasting examination, formulate decisional outcomes predicated upon statistical configurations extracted from instructional datasets. Their decisional thresholds frequently exhibit intricacy, non-linearity, and substantial opacity. A creditworthiness assessment algorithm might inadvertently assimilate correlative patterns between chronological maturity and repayment probability absent explicit programming directives, thereby generating unpremeditated discriminatory outcomes that contravene regulatory stipulations. Laboratory analyses conclusively establish that, despite deliberate elimination of sensitive demographic identifiers from training information repositories, computational decision frameworks nonetheless demonstrate a remarkable capability to infer and reconstitute these prohibited classifications through statistical associations with seemingly unrelated peripheral data elements, thereby engendering substantial compliance vulnerabilities (Datta, A. *et al*., 2016).

Emerging Compliance Risks in AI Systems

The paradigmatic shift toward probabilistic decision formation introduces multifarious compliance vulnerabilities that traditional governance frameworks inadequately address. Unintentional prejudicial outcomes materialize when algorithmic models assimilate and magnify biases embedded within instructional datasets, potentially transgressing anti-discrimination legislative mandates. Scholarly examinations of fairness within classification methodologies have substantiated that particular conceptualizations of fairness demonstrate mathematical incompatibility, thereby generating foundational tensions within compliance obligations (Kleinberg, J. *et al*., 2016). Such incompatibility necessitates that architectural designers formulate explicit determinations regarding which fairness criteria warrant prioritization, frequently absent authoritative regulatory direction.

Interpretability challenges manifest when "black box" computational frameworks generate determinations resistant to straightforward elucidation for regulatory authorities or affected constituencies. Investigative work concerning quantitative input influence has revealed that sophisticated models frequently distribute decisional influence across numerous variables through patterns defying elementary explanation, particularly when variable interactions predominantly determine outcomes (Datta, A. *et al*., 2016). This opacity complicates adherence to regulatory frameworks mandating transparent decision-making processes.

Dynamic computational drift materializes as algorithmic performance characteristics and behavioral patterns transform temporally when data distributions undergo modification, potentially introducing novel compliance complications following deployment. Theoretical frameworks established for classification equivalence insufficiently address the temporal consistency of fairness properties, thereby creating persistent compliance monitoring complexities (Kleinberg, J. *et al*., 2016).

Security vulnerabilities manifest when hostile actors intentionally construct specialized input patterns expressly formulated to manipulate AI systems into producing outputs that violate established compliance boundaries. Transparency mechanisms exposing feature influence occasionally facilitate the construction of adversarial examples, circumventing compliance safeguards (Datta, A. *et al*., 2016).

In final consideration, surrogate attribute exploitation arises when computational models inadvertently discover and utilize ostensibly neutral characteristics that indirectly represent

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

protected categories, effectively bypassing explicit regulatory safeguards despite formal exclusion of prohibited classification factors. Formal analytical examination of classification systems has demonstrated that, absent meticulous constraints, algorithmic models naturally discover and exploit such proxy relationships (Kleinberg, J. *et al*., 2016). These multidimensional risks experience amplification through operational deployment within dynamic environments where both regulatory requirements and operational contexts undergo continuous evolution.

Table 1: Compliance Implementation: Traditional Software vs. AI Systems (Kleinberg, J. *et al*., 2016; Datta, A. *et al*., 2016)

Compliance Aspect	Implementation
Traditional Software	Deterministic, rule-based logic
Machine Learning Systems	Probabilistic pattern inference
Transparency	Explicit vs. opaque
Protected Attributes	Direct exclusion vs. reconstruction
Governance	Established vs. novel approaches

ARCHITECTURAL PATTERNS FOR COMPLIANCE-AWARE AI

Pre-processing Compliance Layers

Pre-computational filtering mechanisms function as selective barriers and transformative agents, ensuring that data traversing into ML processing sequences satisfies regulatory mandates. Input verification checkpoints authenticate data against legislative directives prior to model admission. These verification junctures confirm age declarations or inspect for mandatory consent indicators, thereby preventing non-conformant information from infiltrating analytical pipelines. This methodological approach harmonizes with explicability entitlements codified within contemporary data protection statutes, wherein input validation constitutes the initial phase in guaranteeing comprehensible algorithmic determinations (Wachter, S. *et al*., 2017).

Privacy-maintaining transformational procedures have materialized as indispensable structural elements within compliance-conscious architectural frameworks. Methodologies including differential privacy calculus, federated computational distribution, and homomorphic cryptographic processing enable machine learning infrastructures to extract patterns from confidential information while preserving alignment with privacy statutes. These procedural techniques uphold both explicability rights and erasure entitlements by constraining direct engagement with personal identifiers while facilitating model development (Wachter, S. *et al*., 2017).

Prejudicial pattern identification and remediation frameworks constitute fundamental pre-processing safeguards addressing discriminatory hazards before influencing model formation. These approaches confront interpretational difficulties recognized within contemporary machine learning configurations, wherein intricate models potentially assimilate problematic correlations resistant to post-training detection (Lipton, Z. C. 2018).

Regulatory contextual enrichment involves appending compliance-pertinent descriptors to data elements, preserving contextual integrity throughout processing sequences. This approach amplifies model comprehensibility by maintaining contextual indicators necessary for generating meaningful elucidations of algorithmic determinations as mandated by regulatory frameworks such as GDPR (Wachter, S. *et al*., 2017).

Compliance-Aware Model Design

Algorithmic constructs themselves permit compliance-oriented architectural formulation through diverse structural approaches. Constrained optimization methodologies incorporate regulatory stipulations directly within training objective calculations. This approach reconciles tensions between performance metrics and interpretability considerations highlighted within model transparency investigations (Lipton, Z. C. 2018).

Transparent architectural configurations offer alternative pathways toward compliance-conscious design. Certain algorithmic frameworks, including rule-based mechanisms, decision-tree structures, and sparse linear formulations, deliver enhanced decisional transparency. These approaches reflect growing scholarly recognition that retrospective explanations exhibit inherent limitations and that comprehensibility warrants integration within foundational model architecture (Lipton, Z. C. 2018).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Equity-conscious learning procedures, including adversarial debiasing techniques and fairness constraints, help ensure models satisfy equitable treatment requirements during formation. These methodologies facilitate the generation of counterfactual explanations demonstrating how altered inputs would produce different outcomes, thereby satisfying regulatory mandates for meaningful elucidation of automated decisional logic (Wachter, S. *et al*., 2017).

Regulatory attribute engineering involves the explicit incorporation of compliance-relevant information as features within model architectures. This approach enhances the capacity to generate contrastive explanations that scholarly investigations suggest most effectively satisfy both regulatory mandates and user comprehension requirements (Wachter, S. *et al*., 2017).

Post-processing Governance Controls

Post-computational governance layers function as protective mechanisms verifying and adjusting algorithmic outputs before reaching end-users or downstream systems. Output verification components evaluate model predictions against compliance directives, filtering or highlighting potentially non-conformant results. This approach addresses interpretability limitations within complex models by enforcing compliance irrespective of model transparency (Lipton, Z. C. 2018).

Confidence threshold establishment implements minimum certainty requirements for high-consequence determinations, ensuring human evaluation of uncertain cases. This mechanism acknowledges machine learning interpretability constraints while providing practical safeguards for consequential decisional contexts (Lipton, Z. C. 2018).

Explainability encapsulation generates interpretable justifications for model determinations, satisfying regulatory transparency requirements. These components implement counterfactual explanation methodologies, which scholarly investigations suggest can satisfy legal mandates for meaningful information regarding algorithmic decisions without necessitating comprehensive disclosure of internal computational processes (Wachter, S. *et al*., 2017).

Regulatory precedence rules establish explicit operational logic capable of superseding model predictions when compliance requirements necessitate specific outcomes. This approach recognizes that interpretability transcends technical challenges to encompass alignment between system behavior and human-regulatory expectations (Lipton, Z. C. 2018).

Table 2: Architectural Patterns for Compliance-Aware AI (Wachter, S. *et al*., 2017; Lipton, Z. C. 2018)

Compliance Layer	Implementation
Pre-processing	Input verification, privacy-preserving transformations
Model Design	Constrained optimization, interpretable architectures
Post-processing	Output verification, confidence thresholds
Explainability	Counterfactual explanations, regulatory precedence
Metadata	Contextual enrichment, regulatory attribute engineering

RUNTIME COMPLIANCE MONITORING AND ENFORCEMENT

Real-time Compliance Monitoring

Perpetual surveillance stands fundamentally essential for maintaining legal conformity across dynamically shifting computational environments where underlying data patterns and governmental requirements continually transform throughout operational lifespans. Compliance metric observation facilitates systematic tracking of critical regulatory indicators during operational execution, affording preemptive identification of potential infractions. This surveillance methodology correlates with scholarly recommendations concerning the establishment of verifiable assertions within artificial intelligence infrastructures, wherein persistent verification proves crucial for sustaining trustworthiness and regulatory conformity (Brundage, M. *et al*., 2020).

Anomalous pattern recognition mechanisms employ machine learning methodologies to discern irregular behavioral signatures potentially indicative of compliance transgressions. These infrastructures detect nuanced non-conformance patterns that might otherwise remain unobserved until formal regulatory examination, thereby bolstering institutional frameworks requisite for responsible algorithmic governance (Brundage, M. *et al*., 2020).

Computational drift surveillance capacities permit organizations to recognize when algorithmic models commence deviation from initial

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

behavioral parameters, potentially undermining compliance assurances. Systematic observation for conceptual drift, data distribution shifts, and performance alterations assists identification of circumstances wherein models potentially violate compliance stipulations, triggering preemptive intervention before regulatory transgressions materialize. This harmonizes with recommended methodologies for maintaining algorithmic consistency with compliance expectations throughout operational lifecycles (Gebru, T. *et al*., 2021).

Regulatory evolution monitoring frameworks track progressive legal requirement modifications and evaluate consequential implications for deployed computational models. These systems analyze regulatory amendments, assess potential ramifications for operational systems, and highlight circumstances wherein model behavior potentially diverges from updated legislative frameworks. This capability mirrors the necessity for continuous assessment of artificial intelligence systems against evolving standards as emphasized within frameworks addressing responsible technological development (Brundage, M. *et al*., 2020).

Adaptive Compliance Controls

Execution environments necessitate adaptation to shifting compliance contexts through flexible control architectures. Context-sensitive serving technologies permit machine learning infrastructures to modulate compliance parameters according to situational variables, including user jurisdictional location, applicable regulatory frameworks, and detected risk quotients. This dynamic methodology supports transparent documentation of system capabilities and constraints recommended for responsible artificial intelligence deployment (Gebru, T. *et al*., 2021).

Dynamic policy implementation engines operationalize regulatory requirements without necessitating model retraining. This capability facilitates expeditious response to regulatory modifications while preserving operational continuity, supporting institutional verification mechanisms requisite for sustained compliance (Brundage, M. *et al*., 2020).

Graceful functionality reduction mechanisms furnish fallback alternatives when compliance certainty diminishes. Such methodologies transition toward restrained though regulation-conformant computational pathways when confidence metrics deteriorate, acknowledging the fundamental necessity for algorithmic frameworks to function strictly within documented performance parameters as highlighted throughout ethical computing guidelines (Brundage, M. *et al*., 2020).

Distributed compliance architectures facilitate decentralized enforcement of jurisdiction-specific mandates. Within these frameworks, compliance requirements undergo localized implementation predicated upon jurisdiction-specific directives, with appropriate governance ensuring comprehensive oversight. This approach aligns with recommendations concerning transparent documentation of operational boundaries and contextual variables influencing system behavior (Gebru, T. *et al*., 2021).

These runtime compliance capabilities collectively empower organizations to maintain continuous regulatory alignment within dynamic operational environments. Rather than conceptualizing compliance as momentary certification, these approaches acknowledge that maintaining regulatory adherence demands perpetual vigilance and adaptive response. This perspective reflects the understanding that responsible artificial intelligence necessitates not merely initial verification but continuous monitoring and adjustment as both technological systems and regulatory expectations undergo progressive evolution (Brundage, M. *et al*., 2020; Gebru, T. *et al*., 2021).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

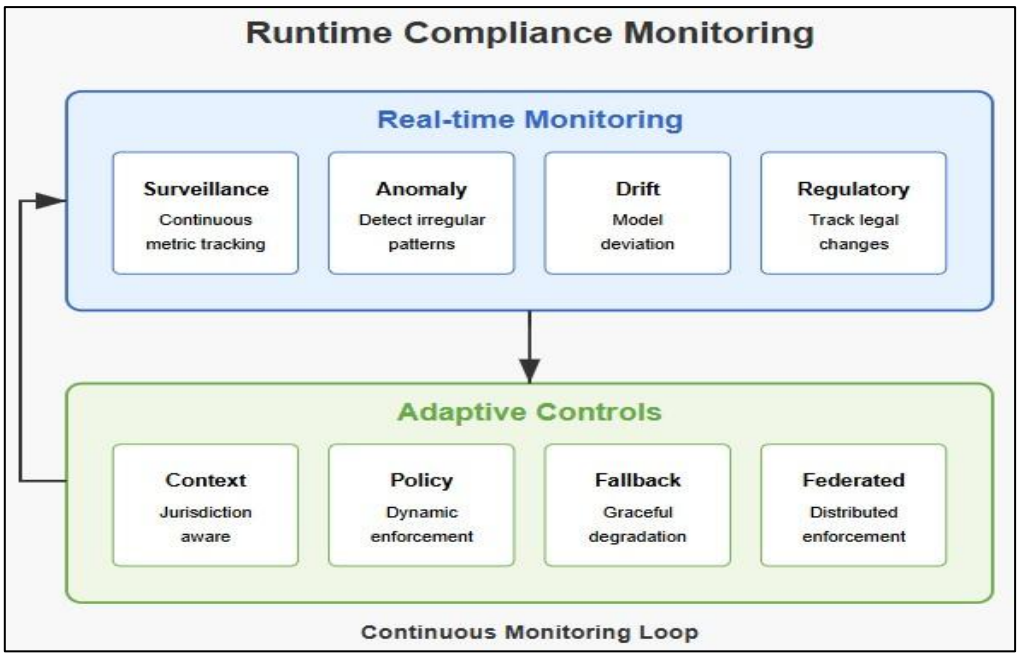


Fig 1: Runtime Compliance Monitoring Framework (Brundage, M. *et al*., 2020; Gebru, T. *et al*., 2021)

IMPLEMENTING COMPLIANCE-AWARE AI PIPELINES

Organizational Frameworks

Successful implementation of compliance-aware AI systems requires appropriate organizational structures that integrate technical and regulatory expertise. Compliance by Design Teams represent a foundational approach, bringing together cross-functional expertise, including ML engineers, legal experts, and compliance officers from project inception. These integrated teams enable regulatory considerations to influence architectural decisions during the formative stages of system design, similar to how model cards promote transparency by documenting key information from the beginning of development (Dalmia, P. 2021).

Model Risk Management frameworks provide formal governance processes for assessing compliance risks throughout the ML lifecycle. These frameworks apply systematic risk assessment methodologies to each stage of the model lifecycle, from data acquisition through deployment and monitoring, addressing the opacity concerns that arise in complex ML systems (Sullivan, E. 2022).

Clear Accountability structures establish specific responsibilities for compliance at each pipeline stage. These accountability structures ensure that compliance considerations receive appropriate attention and resources during each phase of development and operation, supporting the transparency goals emphasized in model card frameworks (Dalmia, P. 2021).

Documentation Requirements establish standards for capturing compliance-relevant information throughout the development process. This documentation provides critical evidence of compliance intent and implementation for both internal governance and external regulatory review, aligning with the structured transparency approach promoted in model card methodologies (Dalmia, P. 2021).

Technical Implementation Patterns

Several technical approaches enable the practical implementation of compliance-aware AI systems. Pipeline Orchestration tools provide mechanisms to enforce compliance checks at each stage of ML workflows. These orchestration systems enforce dependency relationships between compliance verification and subsequent pipeline stages, preventing n

on-compliant artifacts from progressing, thus addressing the epistemic opacity concerns inherent in complex ML systems (Sullivan, E. 2022).

Feature Stores with Compliance Metadata enable centralized management of features with their associated regulatory constraints. These specialized repositories track regulatory metadata alongside feature values, enabling consistent enforcement of usage restrictions and documentation requirements, supporting the contextual information needs identified in model card frameworks (Dalmia, P. 2021).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Model Cards and Datasheets provide standardized documentation templates for capturing compliance-relevant information about models and datasets. These structured documents ensure consistent recording of information critical for compliance evaluation, including intended use cases, performance characteristics, training data attributes, and known limitations, directly addressing the transparency challenges in machine learning (Dalmia, P. 2021).

Compliance as Code approaches express regulatory requirements as executable code that integrates with CI/CD pipelines. This approach transforms regulatory requirements from static documentation into active verification mechanisms that operate continuously throughout the development lifecycle, helping to mitigate the procedural opacity identified in machine learning workflows (Sullivan, E. 2022).

Containerized Compliance Environments leverage containerization technologies to ensure consistent enforcement of compliance rules across environments. These approaches ensure that compliance controls remain consistent across development, testing, and production environments, addressing the replicability challenges that contribute to ML system opacity (Sullivan, E. 2022).

Case Studies

The following case studies illustrate compliance-aware AI in practice across diverse regulatory contexts. In financial services, institutions have implemented credit scoring systems incorporating explicit age verification, anti-discrimination controls, and explainability wrappers to meet regulatory requirements. These implementations address the transparency concerns emphasized in model card frameworks, particularly for high-stakes decision systems (Dalmia, P. 2021).

Healthcare organizations have deployed clinical decision support systems implementing HIPAA compliance through privacy-preserving training techniques and appropriate access controls. These systems demonstrate how addressing multiple forms of opacity can be essential in regulated environments where both privacy and explainability are required (Sullivan, E. 2022).

Content moderation systems have successfully incorporated embedded age verification and jurisdiction-specific content policies. These implementations reflect the context-specific documentation approach advocated in model card frameworks, where intended uses and limitations are clearly specified (Dalmia, P. 2021).

Autonomous vehicle systems have implemented perception frameworks with safety-critical compliance controls and rigorous audit trails for regulatory approval. These implementations address both the technical and social dimensions of opacity in complex systems, creating accountability mechanisms that support regulatory oversight in high-risk domains (Sullivan, E. 2022).

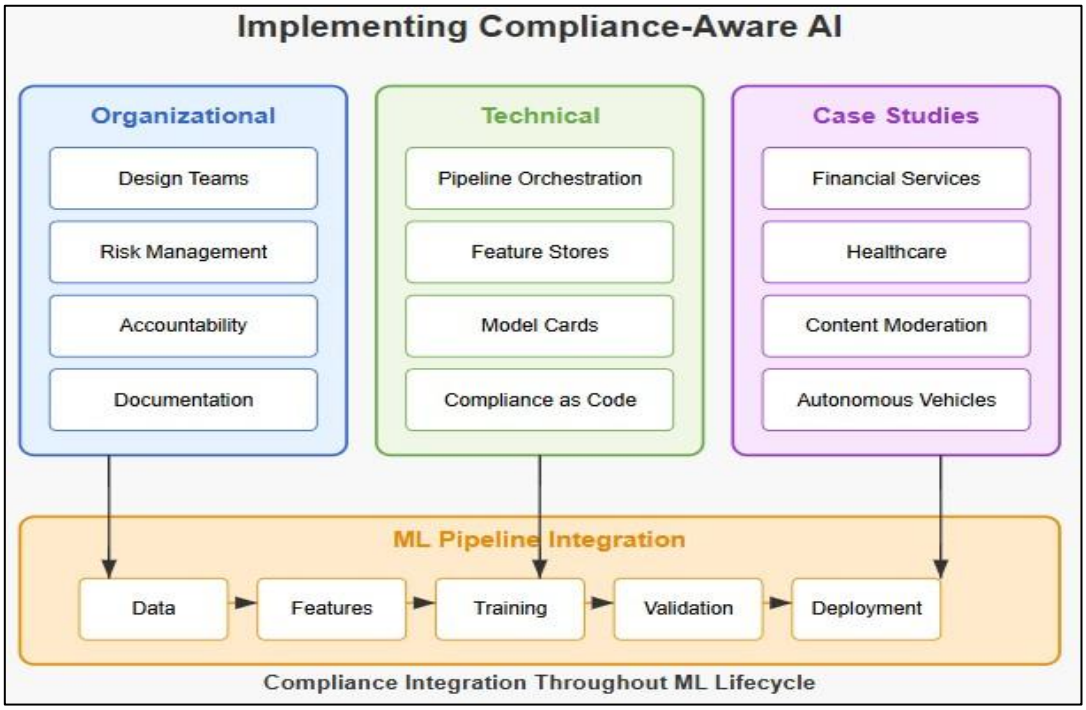


Fig 2: Implementing Compliance-Aware AI Pipelines (Dalmia, P. 2021; Sullivan, E. 2022)

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

CONCLUSION

As algorithmic infrastructures become progressively interwoven within mission-critical applications throughout regulated industrial domains, the imperative of ensuring regulatory conformity transforms from an ancillary consideration to a fundamental design prerequisite. The architectural configurations and methodological frameworks delineated herein proffer a structural approach for embedding legislative logic directly within computational learning sequences, addressing distinctive compliance challenges presented by probabilistic algorithmic systems. Through implementation of compliance safeguards across multiple strata—spanning pre-computational filtration mechanisms through post-computational verification layers and operational monitoring infrastructures—technological practitioners can construct systems maintaining regulatory alignment despite engagement with intricate, dynamic, or inscrutable computational models. Such approaches facilitate innovation while honoring legitimate regulatory parameters that safeguard consumers, uphold equitable treatment, and preserve societal confidence. For product development collectives navigating heavily regulated environments, the pivotal realization emerges that regulatory stipulations warrant conceptualization not as constraints demanding minimal satisfaction, but rather as design principles capable of enhancing comprehensive system quality and dependability. By embracing compliance-conscious design from inception, organizations can circumvent costly remediation endeavors while constructing technological systems embodying both innovative advancement and responsible governance.

REFERENCES

1. Hacker, P., Naumann, F., Friedrich, T., Grundmann, S., Lehmann, A., & Zech, H. "AI compliance–challenges of bridging data science and law." *ACM Journal of Data and Information Quality (JDIQ)* 14.3 (2022): 1-4.
2. Google.com, "ML pipelines." https://developers.google.com/machine-learning/managing-ml-projects/pipelines
3. Kleinberg, J., Mullainathan, S., & Raghavan, M. "Inherent trade-offs in the fair determination of risk scores." *arXiv preprint arXiv:1609.05807* (2016).
4. Datta, A., Sen, S., & Zick, Y. "Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems." *2016 IEEE symposium on security and privacy (SP)*. IEEE, (2016).
5. Wachter, S., Mittelstadt, B., & Russell, C. "Counterfactual explanations without opening the black box: Automated decisions and the GDPR." *Harv. JL & Tech.* 31 (2017): 841.
6. Lipton, Z. C. "The mythos of model interpretability: In machine learning, the concept of interpretability is both important and slippery." *Queue* 16.3 (2018): 31-57.
7. Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., ... & Anderljung, M. "Toward trustworthy AI development: mechanisms for supporting verifiable claims." *arXiv preprint arXiv:2004.07213* (2020).
8. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Iii, H. D., & Crawford, K. "Datasheets for datasets." *Communications of the ACM* 64.12 (2021): 86-92.
9. Dalmia, P. "Model Cards for Model Reporting." *Medium*, (2021). https://priyanka-dalmia.medium.com/model-cards-for-model-reporting-3d934a67d28
10. Sullivan, E. "How values shape the machine learning opacity problem." *Scientific understanding and representation*. Routledge, (2022). 306-322.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Piratiyath, H. "Compliance-aware AI: Embedding Regulatory Logic into Machine Learning Pipelines" *Sarcouncil Journal of Engineering and Computer Sciences* 4.9 (2025): pp 40-47.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher