Review

Impact of EU Laws on the Adoption of AI and IoT in Advanced Building Energy Management Systems: A Review of Regulatory Barriers, Technological Challenges and Economic Opportunities

Bo Nørregaard Jørgensen * and Zheng Grace Ma

Posted Date: 9 May 2025

doi: 10.20944/preprints202505.0702.v1

Keywords: building energy management systems; artificial intelligence; internet of things; EU regulations; smart buildings

Review

Impact of EU Laws on the Adoption of AI and IoT in Advanced Building Energy Management Systems: A Review of Regulatory Barriers, Technological Challenges and Economic Opportunities

Bo Nørregaard Jørgensen * and Zheng Grace Ma

SDU Center for Energy Informatics, Maersk Mc-Kinney Moller Institute, The Faculty of Engineering, University of Southern Denmark

* Correspondence: bnj@mmmi.sdu.dk; Tel.: +4529125778

Abstract: The integration of Artificial Intelligence (AI) and the Internet of Things (IoT) in Building Energy Management Systems (BEMS) offers transformative potential for improving energy efficiency, enhancing occupant comfort, and supporting grid stability. However, the adoption of these technologies in the European Union (EU) is significantly influenced by a complex regulatory landscape, including the EU AI Act, the General Data Protection Regulation (GDPR), the EU Cybersecurity Act, and the Energy Performance of Buildings Directive (EPBD). This review systematically examines the legal, technological, and economic implications of these regulations on AI- and IoT-driven BEMS. First, we identify legal and regulatory barriers that may hinder innovation, such as data protection constraints, cybersecurity compliance, liability concerns, and interoperability requirements. Second, we explore technological challenges in designing regulatory-compliant AI and IoT solutions, focusing on data privacy-preserving architectures (e.g., edge computing vs. cloud processing), explainability requirements for AI decision-making, and cybersecurity resilience. Finally, we highlight the economic opportunities that arise from regulatory alignment, demonstrating how compliant AI and IoT-based BEMS can unlock energy savings, operational efficiencies, and new business models in smart buildings. By synthesizing current research and policy developments, this review provides a comprehensive framework for understanding the intersection of regulatory requirements and technological innovation in AI-driven building management. We discuss strategies to navigate regulatory constraints while leveraging AI and IoT for energy-efficient, intelligent building operations. The insights presented aim to guide researchers, policymakers, and industry stakeholders in advancing regulatory-compliant BEMS that balance innovation, security, and sustainability.

Keywords: building energy management systems; artificial intelligence; internet of things; EU regulations; smart buildings

1. Introduction

The convergence of artificial intelligence AI and the Internet of Things IoT in advanced Building Energy Management Systems BEMS promises significant improvements in energy efficiency, occupant comfort, and grid stability [1], [2]. AI-driven BEMS can optimize heating, ventilation, and air conditioning HVAC, lighting, and other building systems in real-time by learning usage patterns and preferences, yielding substantial energy savings studies report 20–40% reductions while maintaining or even enhancing indoor comfort [1]. IoT sensors further enable these systems to respond dynamically to occupancy and participate in demand response programs for balancing supply and demand with minimal impact on occupants [2]. These capabilities position smart BEMS as key enablers for sustainable buildings and smarter grids, where buildings not only consume but also actively manage and even store energy to support overall grid stability. European initiatives such as BUILD UP's overview of smart technologies [3], the Digital Single Market strategy for IoT [4], and Horizon-2020 pilots on interoperable smart homes and grids [5] underscore the policy momentum.

In Europe, the regulatory landscape is rapidly evolving to both encourage and govern the adoption of AI/IoT technologies in smart buildings. The European Union's General Data Protection Regulation GDPR imposes strict requirements on the handling of any personal data collected by building sensors e.g. occupancy, environmental conditions [6]. The forthcoming EU Artificial Intelligence Act AI Act will be the first comprehensive AI law, classifying certain AI applications as "high-risk" and mandating risk assessments, transparency, and human oversight for those systems [7], [8]. Cybersecurity is another focal point: the EU Cybersecurity Act 2019 established a framework for voluntary cybersecurity certification of ICT products [9], including IoT devices [10], and a proposed Cyber Resilience Act will soon introduce mandatory security-by-design requirements for products with digital elements covering IoT hardware and software [10], [11]. In the building domain, the Energy Performance of Buildings Directive (EPBD) has been revised to promote smart technologies. For example, it requires installation of building automation and control systems BACS in large non-residential buildings by 2025, recognizing that advanced control and monitoring can drastically cut energy waste [12]. Meanwhile, the Network and Information Security Directive NIS, updated as NIS2 extends cybersecurity obligations to operators of essential services, which can include building infrastructure in critical sectors, e.g. HVAC systems in hospitals or data centers, enforcing risk management, incident reporting, and supply chain security for smart building systems [13], [14]. Other EU initiatives, such as the Data Act, further shape the landscape by clarifying data access and sharing rights for IoT device data including building sensor data, aiming to stimulate innovation while protecting user interests [15], [16], [17].

Amid these developments, there is a clear need to understand how EU regulations impact the design and deployment of AI- and IoT-enabled BEMS. On one hand, policy measures like the EPBD actively encourage smart building upgrades to achieve climate goals. On the other hand, laws on data privacy, AI safety, and cybersecurity impose compliance obligations that could act as barriers or challenges to adoption. This scoping review explores three interrelated aspects of this topic: the legal barriers introduced by EU regulations, the technological challenges in creating compliant AI/IoT BEMS solutions, and the economic opportunities arising from regulatory alignment. The objectives are to identify how current and upcoming EU laws affect AI and IoT integration in BEMS, what technical hurdles must be overcome to meet these legal requirements, and what economic or market openings exist for solutions that successfully navigate the regulatory environment.

Accordingly, the review is guided by the following key research questions: 1 How do EU regulations impact the adoption of AI and IoT in advanced BEMS in terms of both constraints and drivers? 2 What technological challenges do engineers and developers face in designing BEMS that comply with data protection, AI governance, and cybersecurity requirements? 3 What economic opportunities emerge from deploying regulatory-compliant AI/IoT-based BEMS, such as energy cost savings, new value streams, or competitive advantages? By addressing these questions, the review aims to map the current knowledge on policy impacts in this domain and highlight areas where further research or policy action is needed.

2. Methodology

This review was conducted as a scoping review following the PRISMA-ScR Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews guidelines [18]. A scoping review approach was chosen because our aim is to map the interdisciplinary evidence on law, technology, and economics in the context of smart building systems, rather than to test a narrow hypothesis. We followed a predefined protocol outlining the core elements of the PRISMA-ScR framework: defining the scope of inquiry, identifying relevant studies, selecting studies, charting the data, and collating, summarizing, and reporting results. Below, we detail how each step was implemented.

Eligibility Criteria: We included a broad range of source types to capture the multifaceted nature of the topic. Eligible sources encompassed peer-reviewed academic literature e.g. journal articles, conference papers as well as grey literature such as EU policy documents, directives and regulations, technical reports from agencies like ENISA for cybersecurity, industry white papers, and relevant standards or guidance. Inclusion was limited to sources addressing building energy management or smart building technologies in conjunction with EU regulations or requirements on AI, data, or security. We included studies focusing on energy efficiency, demand response, or smart building controls only if they discussed regulatory or compliance aspects. Conversely, we included legal and policy analyses e.g. GDPR or AI Act discussions only if they were applied in the context of IoT/AI systems or smart buildings. Publications had to be in English and dated within approximately the last 10 years 2015–2025, a period which covers the introduction of GDPR, the latest EPBD revisions, and the emergence of AI/IoT regulation in the EU. Earlier seminal works were considered for background if necessary.

Information Sources and Search Strategy: We performed comprehensive searches across multiple databases and repositories to ensure coverage of both academic and regulatory literature. The academic databases Web of Science WoS, Scopus, and IEEE Xplore were queried for peer-reviewed papers. Key search terms included combinations of “smart building*” OR “building energy management” OR EPBD AND “AI” OR “artificial intelligence” OR “IoT” OR “Internet of Things” AND “EU” OR “Europe” AND GDPR OR “AI Act” OR “Cybersecurity Act” OR NIS2. To capture relevant legal and policy documents, we searched the EUR-Lex database for EU directives/regulations texts and communications and the European Commission’s websites for policy reports or guidelines e.g. documentation on the AI Act, the EPBD, the NIS Directive, etc. We also consulted the ENISA European Union Agency for Cybersecurity repository for reports on IoT and smart infrastructure security. Additional industry insights were sought via general web search, which led to sources like the Building Services and smart controls industry blogs, and law firm commentaries on emerging regulations. Table 1. lists the optimized search string for each of the data sources.

Table 1. Search strings and search engines for each of the data sources.

Web of Science, Scopus, IEEE Xplore	autoresearch.sdu.dk ("smart building*" OR "intelligent building*" OR "Smart home*" OR "building energy management") AND (AI OR "artificial intelligence" OR IoT OR "Internet of Things") AND (EU OR “Europe*”) AND (Privacy OR GDPR OR "AI Act" OR "Cybersecurity Act" OR NIS2)
EUR-Lex	Google site:eur-lex.europa.eu ("smart building*" OR "intelligent building*" OR "Smart home*" OR "building energy management") (AI OR "artificial intelligence" OR IoT OR "Internet of Things") (EU OR “Europe*”) (Privacy OR GDPR OR "AI Act" OR "Cybersecurity Act" OR NIS2)
ENISA	Google site:www.enisa.europa.eu ("smart building*" OR "intelligent building*" OR "Smart home*" OR "building energy management") (AI OR "artificial intelligence" OR IoT OR "Internet of Things") (EU OR “Europe*”) (Privacy OR GDPR OR "AI Act" OR "Cybersecurity Act" OR NIS2)
Web search	Google site:europa.eu ("smart building*" OR "intelligent building*" OR "Smart home*" OR "building energy management") (AI OR "artificial intelligence" OR IoT OR "Internet of Things") (EU OR “Europe*”) (Privacy OR GDPR OR "AI Act" OR "Cybersecurity Act" OR NIS2)

Selection of Sources: All search results were imported into a reference management tool, and duplicates were removed. We then screened titles and abstracts or executive summaries, in the case of reports against the eligibility criteria. At this stage, we excluded obviously irrelevant items e.g.

doi:10.20944/preprints202505.0702.v1

papers on AI in buildings with no mention of regulations, or papers on EU data law with no connection to buildings. The remaining sources underwent full-text review to determine inclusion. Figure 1 illustrates the study selection process as a PRISMA flowchart, summarizing the number of records identified, screened, excluded, and included at each step. In total, we included approximately 64 sources, comprising about 34 peer-reviewed articles and 30 reports or legal documents, as listed in table 2.

Table 2. Summary of source selection and the number of identified, screened, and included records.

Source	Identification	Screening	Included
Web of Science, Scopus, IEEE Xplore	61	40	34
EUR-Lex	195	Top 50	20
ENISA	14	14	2
Web search	1590	Top 100	8

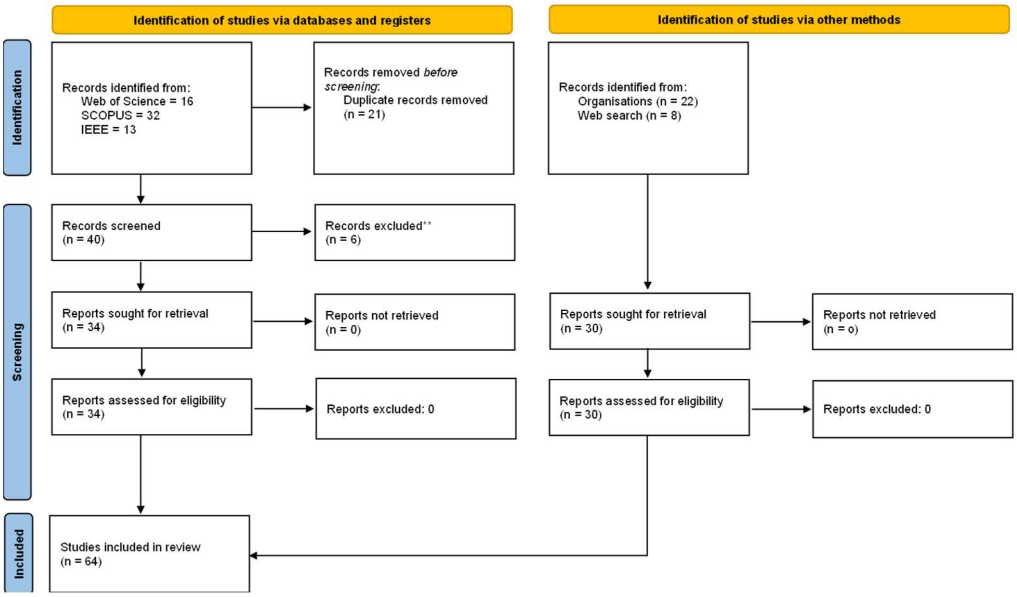

Figure 1. The PRISMA-ScR flow diagram is based on the source counts listed in Table 2.

Data Extraction and Synthesis: From each included source, relevant data were charted using a structured form. We extracted information on: a legal or regulatory aspects discussed e.g. specific laws like GDPR or AI Act, compliance challenges noted, legal recommendations, b technological aspects e.g. the architecture of the BEMS, use of AI/ML techniques, data flows, security measures, etc., especially in relation to meeting or being hindered by regulations, and c economic or market aspects e.g. costs, benefits, business opportunities, incentives related to regulatory compliance or non-compliance. We then conducted a thematic analysis, grouping findings into the three main themes of this review: legal barriers, technological challenges, and economic opportunities. Within each theme, sub-themes were identified inductively. For instance, under legal barriers, distinct sub-topics such as data privacy, AI transparency requirements, cybersecurity mandates, interoperability standards, and liability concerns emerged. Similarly, under technological challenges we noted sub-themes like data management in edge vs cloud, explainable AI, cybersecurity resilience, and integration/interoperability. The economic opportunity's theme covered sub-themes like energy cost savings, operational efficiency, market growth for smart building tech, and innovation driven by compliance. We synthesized the findings narratively, with emphasis on how literature answers the research questions. Where appropriate, we also tabulated certain information – for example, a summary of key EU regulations and their known or expected impacts on BEMS – to provide the reader with a clear overview of the regulatory landscape.

3. Results

The search and analysis yielded a panorama of insights across legal, technical, and economic dimensions. In this section, we present the results in three parts: 3.1 Legal barriers, i.e. how EU laws and regulations pose challenges or set conditions for AI/IoT adoption in BEMS; 3.2 Technological challenges in developing and deploying BEMS that meet these regulatory requirements; and 3.3 Economic opportunities that arise from compliance and innovation in this space. Throughout, we highlight evidence from the literature to answer the research questions.

3.1. Legal Barriers and Regulatory Constraints

Data Privacy and GDPR Compliance: A foremost legal barrier is ensuring compliance with the GDPR in AI- and IoT-enabled BEMS. Smart building systems inevitably collect large volumes of data in terms of occupancy information, temperature preferences, ventilation needs, collectively providing patterns that could identify an individual's routine. Under the GDPR, many of these data points especially when linked or inferable to individuals or tenants are considered personal data, triggering strict requirements for lawful processing, security, and data minimization [6]. A recurring theme in the literature is that the GDPR, while comprehensive, was not written with smart buildings in mind, making its application to BEMS somewhat unclear [6]. For instance, energy usage data or occupancy sensor readings might be anonymous in isolation, and thus outside GDPR scope, but when combined e.g. energy patterns revealing when a person is at home, they can become personally identifiable. This ambiguity creates compliance uncertainty as building operators are unsure how to implement consent, data anonymization, or deletion in practice. Abu Bakar et al. 2024 note that many researchers and operators "turn to existing privacy regulations such as the GDPR for guidance" but that "applying the GDPR to energy-efficient smart building infrastructure is not straightforward" [6]. Challenges include difficulty in obtaining valid consent from building occupants for data collection in a shared environment, determining the data controller building owner vs. service provider, and implementing individuals' rights like data access or erasure in systems that aggregate sensor data [19], [20]. Recent analyses of smart-device privacy policies reveal vagueness about third-party data sharing [21], and user-centric frameworks have been proposed to give occupants greater control [22], [23]. Solutions such as blockchain-based ledgers for verifiable retention are also being explored [24], alongside cloud-side enforcement mechanisms like IoT Expunge [25]. Looking forward, combined GDPR-plus AI-Act obligations feature prominently in projections of the EU privacy landscape for 2025 [17]. Thus, GDPR's stringent privacy protections, while essential for user trust, represent a legal hurdle that BEMS developers must carefully navigate, often requiring additional data handling features that add complexity.

EU AI Act – Transparency, Accountability and Risk Management: The proposed EU AI Act AIA is poised to introduce a new layer of legal obligations for BEMS that incorporate AI. Under the current draft of the Act, AI systems are classified by risk; some applications in BEMS may be deemed high-risk, especially if they directly affect safety for example, an AI controlling critical ventilation in a healthcare facility or significantly impact occupants' rights such as algorithms that might inadvertently discriminate in heating provision. If an AI-driven BEMS or component is classified as high-risk, the Act will require compliance with numerous requirements before it can be placed on the market [8]. These include conducting a conformity assessment and implementing a risk management system throughout the AI's lifecycle [7], [8]. Notably, the Act mandates transparency and explainability for high-risk AI. The system must provide clear information on its functionality and limitations, and logs must be kept ensuring traceability of decisions [8]. For BEMS, this could mean developers need to include explanation modules for how the AI is adjusting building controls, especially if those adjustments affect occupants e.g. why the system chose to curtail heating in a room at a given time. Ensuring such explainability can be technically challenging, especially for complex machine learning models, and may require choosing more interpretable algorithms over more accurate but black box models. Energy-sector–specific trustworthy-AI evaluation frameworks such as E-TAl are emerging to operationalize these duties [26]. The AI Act also emphasizes human oversight, meaning that operators should be able to monitor AI decisions and intervene or override when necessary [8]. In a building context, this raises questions of liability and operational practicality, as facilities managers might need new training or interfaces to supervise AI controls. Another critical requirement is robustness and cybersecurity for AI systems [8]. The Act will oblige manufacturers to secure AI models against manipulation or misuse, which intersects with IoT device security since an attacker could tamper with sensor inputs or actuator commands. In summary, the AI Act, once in force, will act as a legal gatekeeper for AI-enabled BEMS, as solutions will need to be designed upfront to meet documentation, transparency, and risk mitigation standards [8]. While this raises the bar for quality and trustworthiness, it also imposes additional development and certification costs. Early analyses suggest that IoT/BEMS manufacturers should start aligning with these requirements in the design phase to avoid expensive retrofits later [8].

Cybersecurity Requirements NIS Directive and Cybersecurity Act: As buildings become integrated into critical connected infrastructure, the EU has introduced several cybersecurity regulations that significantly affect the deployment and operation of advanced BEMS. The original NIS Directive 2016 and its successor, the NIS2 Directive (EU 2022/2555), impose stringent cybersecurity obligations on operators of essential and important entities, which now explicitly include facilities that manage smart building systems, such as airports, hospitals, data centers, and other critical infrastructure [13], [14]. Consequently, building automation and management systems (BAS/BMS) used in these settings must be incorporated into broader cybersecurity risk assessments, incident reporting protocols, and compliance regimes. Key requirements under NIS2 include conducting regular risk analyses, ensuring network segmentation between building systems and corporate IT networks, securing remote access mechanisms, and maintaining an actionable incident response plan [14]. Organizations are also obligated to report significant cybersecurity incidents, such as BEMS-related breaches, within 24 to 72 hours, depending on severity. The directive also places strong emphasis on supply chain security, compelling building operators to ensure that vendors and IoT device suppliers adhere to cybersecurity best practices. This includes the use of certified components, timely deployment of security patches, and elimination of insecure practices such as hard-coded passwords [14]. Complementing NIS2, the EU Cybersecurity Act provides a framework for voluntary cybersecurity certification schemes across the Union [9]. Although certification is not yet mandatory, schemes for securing IoT devices and digital systems are under development. These could soon become essential, particularly where public procurement or liability standards are involved. Failure to comply with NIS2 obligations can result in penalties of up to 2% of global turnover, creating substantial incentives for compliance [14]. The forthcoming Cyber Resilience Act further strengthens the regulatory landscape by introducing lifecycle security obligations for all products with digital elements, including BEMS and IoT devices [11], [10]. It aims to ensure that cybersecurity is embedded throughout the product lifecycle, from design to disposal. Supporting these legal frameworks, ENISA has published good-practice guidance specific to smart-home and smart-building environments [27], along with comprehensive threat landscape reports that detail common attack vectors [28]. Additional concerns about unvetted, “rush-to-market” IoT products—highlighted by high-profile ransomware attacks in the hospitality sector—underscore the urgency of regulatory enforcement [29]. Technical frameworks such as SparkXS provide fine-grained access control mechanisms for managing real-time data streams in smart environments [30], while initiatives like the ForeSight project enhance identity and access management for widely used open-source BEMS middleware [31]. Together, these regulatory instruments and best-practice frameworks function as both barriers and catalysts: they elevate the cybersecurity requirements for smart BEMS and increase design complexity, but they also drive innovation towards more resilient, secure, and trustworthy systems that facilitate broader adoption.

Interoperability and Data Sharing Regulations: The EU regulatory framework increasingly emphasizes interoperability and data sharing, both of which are pivotal to the broader adoption and functionality of advanced BEMS. Central to this agenda is the forthcoming Data Act [15], a proposed regulation on harmonized rules for fair access to and use of data, particularly data generated by IoT devices. For the smart building sector, the Data Act establishes data portability rights for building owners and users, enabling them to access and share data from smart devices, such as sensors, thermostats, solar inverters, with third-party service providers of their choice [8], [17]. This aims to foster a dynamic aftermarket of energy management, analytics, and optimization services. However, to comply with these provisions, BEMS and IoT devices must be designed to export data in standardized, machine-readable formats. This effectively transforms interoperability from an engineering ideal into a legal mandate. Manufacturers that previously relied on proprietary data formats must now implement open APIs or interfaces that support secure data portability. This shift can accelerate the integration of AI-driven modules with legacy building systems, improving their performance and adaptability. At the same time, it raises concerns over data security and the viability of data-centric business models that rely on exclusivity. The push for interoperability is reinforced by earlier standardization efforts such as the CEN-CENELEC alignment [5] and industry-led schemas for multi-system communication [32], as well as technical guidance linking standards like ISO 52000 and the Smart Readiness Indicator (SRI) [33], [12], [34]. The SRI, as introduced in the revised Energy Performance of Buildings Directive (EPBD), rewards buildings that demonstrate the ability to adapt operations to occupant needs and external energy signals. Achieving a high SRI score requires IoT systems to interface with grid signals (e.g., for demand response) and benchmarking tools, necessitating support for protocols such as BACnet [35], KNX [36], or OpenADR [37]. Despite its long-term benefits, implementing interoperability poses practical challenges. Many buildings contain a heterogeneous mix of legacy systems and modern IoT devices, complicating unified BEMS integration. Addressing these challenges often requires retrofitting with protocol converters or adopting middleware platforms, which can increase project costs and complexity [2]. Large-scale EU initiatives like "Digitalising the Energy System and InterConnect" demonstrate how these interoperability principles are being piloted and scaled in practice [38], [39].

Liability and Safety Concerns: As AI systems become integral to autonomous decision-making in advanced BEMS, the question of liability and safety becomes increasingly significant. Traditionally, liability for building system failures, such as a thermostat malfunction causing frozen pipes or ventilation issues resulting in health risks, could be attributed either to the manufacturer (under product liability) or the building operator (under negligence). However, the integration of opaque and complex AI decision-making processes complicates these legal boundaries. The European Commission has acknowledged this challenge in its staff working document on liability for emerging digital technologies, which highlights issues related to AI's lack of transparency and predictability [40].

To address these concerns, the EU has proposed two major legislative updates: a revised Product Liability Directive (PLD) [41] and a new AI Liability Directive (AILD) [42], both introduced in 2022 and subject to extensive legal analysis [43]. Under the revised PLD, manufacturers of AI-enabled products, such as smart HVAC or lighting systems, can be held strictly liable for damage caused by defective products, aligning AI systems with existing product safety obligations. Meanwhile, the proposed AILD aims to ease the process for individuals seeking compensation for harm caused by AI systems. Notably, it adjusts the burden of proof, if an AI-controlled BEMS leads to occupant harm, the responsibility may shift to the system's developer or deployer to demonstrate they were not at fault. While these liability directives do not constitute direct regulatory barriers, they introduce legal uncertainties that may deter building owners from fully embracing autonomous AI controls without assurances of insurance coverage and legal clarity. For example, if an AI optimization unintentionally creates a safety hazard, such as turning off lights on an occupied staircase to conserve energy, it remains unclear whether liability would rest with the developer, operator, or the AI system itself. The emerging consensus suggests that accountability will primarily lie with the developer and deployer, incentivizing them to implement safety overrides, conduct rigorous testing, and maintain comprehensive documentation of risk assessments and regulatory compliance. This evolving liability landscape also has implications for product design and deployment strategies. BEMS vendors must prepare to demonstrate adherence to recognized safety and cybersecurity standards to qualify for legal protection under the revised framework. Some experts have advocated for the creation of regulatory sandboxes; that is, controlled environments where AI in buildings can be tested with reduced legal exposure. The AI Act explicitly encourages EU Member States to establish such sandboxes, promoting innovation while managing legal risk [44]. EU liability reforms are reshaping the legal context in which AI-enabled BEMS operate. While these changes promote responsible innovation by establishing clear lines of accountability, they also require system developers and building operators to adopt more rigorous compliance practices, ultimately contributing to safer and more trustworthy smart building environments.

In summary, EU regulations impose a complex array of legal considerations on AI/IoT adoption in BEMS. Data privacy laws require careful data governance and pseudonymization techniques; the AI Act will demand transparency, risk management, and possibly formal certification of AI modules; cybersecurity laws enforce robust protection of systems and supply chains; interoperability mandates push for open standards and data sharing capabilities; and evolving liability doctrines ensure that harm caused by AI/IoT will not go unaddressed. These “barriers” are in many cases deliberate checks and balances, designed to protect citizens’ rights and safety, but they do require significant effort from stakeholders to navigate.

Table 3 summarizes these key legal requirements and their implications for BEMS. The next section examines how these legal drivers translate into technical challenges in system design and implementation.

Table 3. Summary of Relevant EU Regulations Impacting AI and IoT in BEMS.

Regulation	Focus Area	Key Compliance Requirements	Implications for BEMS
General Data Protection Regulation (GDPR)	Data privacy and protection	Lawful basis for data processing, data minimization, anonymization or pseudonymization, consent management, data subject rights	Requires local data processing (edge computing), privacy-by-design architectures, data governance features
Artificial Intelligence Act (draft)	AI safety, transparency, accountability	Risk classification, conformity assessment, transparency and explainability, human oversight, robustness and security	High-risk AI modules in BEMS must meet documentation and traceability requirements; prefer explainable AI
NIS2 Directive	Cybersecurity for critical infrastructure	Risk assessment, incident response plans, network segmentation, secure remote access, supply chain cybersecurity	Requires BEMS cybersecurity hardening; integration of monitoring and alert systems; secured update processes
EU Cybersecurity Act	Cybersecurity certification frameworks	Voluntary certification schemes for ICT products (e.g. IoT devices, software)	Enables BEMS components to be certified for trust; may become essential for public tenders or insurance
Energy Performance of Buildings Directive (EPBD)	Energy efficiency and smart readiness	Smart Readiness Indicator, mandatory BACS for non-residential buildings, energy monitoring and control systems	Drives demand for AI/IoT-enabled BEMS; requires interoperability, performance monitoring, and analytics
Data Act (proposal)	IoT data access and portability	Right for users to access and share IoT data, fair terms for	Requires BEMS to support data export, API development, and standard

		data use, standardization of data formats	interfaces for third-party services
AI Liability Directive (proposal)	Civil liability for AI-based damage	Facilitates damage claims caused by AI; burden of proof adjustments for high-risk AI	Encourages comprehensive logging, risk assessments, and insurance for AI-controlled building functions
Product Liability Directive (revised)	Manufacturer liability for defective products	Strict liability for AI/IoT-based systems causing harm	Requires rigorous product testing, documentation, and defect traceability in BEMS solutions

3.2. Technological Challenges for Compliance

Implementing AI and IoT in BEMS under the shadow of regulatory requirements brings several technical hurdles to the forefront. Developers and engineers must not only solve the usual problems of optimizing energy and comfort, but also embed solutions for privacy, security, and transparency. The following are major technological challenges identified in the literature.

Edge vs. Cloud Computing – Data Localization and Latency: One design decision with regulatory implications in BEMS deployment is whether to perform data processing locally at the edge (e.g. at the building or device level) or remotely in the cloud. Cloud-based BEMS analytics can harness powerful computational resources and aggregate data across multiple sites, potentially yielding richer insights. However, transmitting detailed occupant or building operation data to the cloud raises privacy concerns under the GDPR. Edge computing, by contrast, processes data locally, on-site servers, gateways, or embedded processors, and thereby helps mitigate privacy risks by minimizing the transfer of personal information to external servers [45]. Indeed, edge computing has been highlighted as a way to "temper some of the privacy risks" associated with IoT data by aligning with GDPR's data minimization principle [45]. For example, an edge-based AI can process raw sensor inputs within the building and only transmit anonymized performance metrics to the cloud. In addition to enhancing data protection, edge computing reduces dependency on continuous internet connectivity and can improve latency and responsiveness, key advantages for real-time control scenarios such as HVAC or lighting adjustments. Research has demonstrated the feasibility of privacy-preserving occupancy estimation using embedded edge processors while maintaining high accuracy, further validating the practical potential of edge AI [46]. However, edge architecture introduces a new set of cybersecurity concerns. While distributing processing tasks avoids the concentration of sensitive data in central cloud repositories, it also multiplies the number of potential attack surfaces across building controllers, IoT hubs, and other edge nodes [45]. Each device becomes a possible target, and ensuring security across many distributed endpoints remains a complex challenge. As Swabey notes, insufficiently secured edge infrastructure can expose systems to increased cyber threats [45]. Another trade-off involves computational limitations. Edge devices typically have constrained resources, limiting the size and complexity of AI models that can be deployed locally. This can affect the performance of advanced energy optimization algorithms. To address this, emerging solutions like federated learning are being explored. In federated learning, AI models are trained collaboratively across multiple buildings' local data sets without transferring raw data, hence only model updates are shared. This approach is explicitly recognized as privacy-preserving and potentially "net-positive for privacy" [45]. Hence, the choice between edge and cloud computing is not only a technical matter but a regulatory and security concern. While cloud solutions offer scale and computational power, edge architectures are often better aligned with GDPR requirements and enable real-time responsiveness. Hybrid models that combine localized processing with cloud-based analytics are increasingly favored, offering a compromise that balances privacy, performance, and compliance.

Explainability and Transparency of AI Algorithms: As highlighted in the legal discussion, explainability is not merely a desirable feature but a likely requirement for high-risk AI systems under the forthcoming EU AI Act [8]. In the context of advanced BEMS, implementing explainable AI (XAI) presents substantial technical challenges. Many current AI approaches, such as deep neural networks or advanced reinforcement learning, are considered "black-box" models that do not inherently provide human-understandable justifications for their decisions. Yet, applications like HVAC control, building operators and occupants may expect explanations for AI behavior, particularly when it diverges from anticipated norms. For instance, failing to heat a room to its usual setpoint. To meet this demand, researchers are exploring several strategies. These include substituting or augmenting black-box models with inherently interpretable approaches like decision trees or rule-based systems [8]. One method pairs a complex neural network controller with a simpler surrogate model that approximates its decisions in a human-readable format. For example, "If occupancy is low and energy prices are high, reduce heating by X degrees." Another method is extensive logging of system states and AI decisions, enabling post hoc audits of system behavior. This practice supports regulatory transparency mandates, as the AI Act will require that detailed documentation of a system's logic, training data, and performance metrics be made available to users and regulators [8]. Technically, this implies that BEMS developers must build robust monitoring, logging, and audit mechanisms directly into their AI control software. These logs, potentially containing sensitive operational or occupancy data, must also be stored securely, adding another layer of compliance and system complexity. Furthermore, to prevent unpredictable or opaque system behavior, AI algorithms may require modification to ensure a certain degree of determinism and predictability. Another dimension of explainability is the human-machine interface. Facility managers must be able to understand what the AI is doing and why. This necessitates intuitive dashboards and alert systems that flag unusual decisions and summarize the contributing factors in plain language. However, there is often a trade-off between explainability and performance, as more transparent models tend to be simpler and may not achieve the same level of energy efficiency as opaque high-performance models. Additionally, continuous logging and auditing can slightly impair system responsiveness. To navigate these tensions, best-practice frameworks such as trustworthy-AI checklists for the energy domain have emerged, emphasizing the need for interpretable models, comprehensive audit trails, and structured human oversight [26], [47]. These frameworks guide developers in aligning AI-driven BEMS with both regulatory requirements and stakeholder expectations for transparency and accountability. Balancing performance, interpretability, and compliance is a core design challenge for AI in smart buildings. Achieving this balance is essential for regulatory approval, user trust, and ultimately the scalable deployment of AI-driven energy management solutions.

Cybersecurity and Resilience: Technologically, ensuring cybersecurity in a highly connected Building Energy Management System (BEMS) is among the most demanding challenges in smart building deployment. These systems increasingly integrate operational technology (OT), such as HVAC controllers, sensors, and actuators with traditional IT infrastructure, creating a complex cyber-physical environment. This convergence exposes OT devices, which were historically not designed with strong security, to a broad attack surface. Common vulnerabilities include outdated firmware, default passwords, and unsecured communication protocols. The regulatory push from the NIS2 Directive and the EU Cybersecurity Act reinforces the need for BEMS to implement state-of-the-art cybersecurity controls. This includes multilayered protections: device-level security, network segmentation, and overall system integrity. Certified hardware that supports encryption and authentication at the chip level is becoming essential, particularly as future EU cybersecurity certification schemes are formalized [48]. Network security practices such as zero-trust segmentation, where every device must authenticate continuously and receives only the minimum required access, are now standard [48]. This ensures that, for example, a compromised smart light bulb cannot be used to access critical systems like HVAC controllers or corporate servers [14]. Securing remote access is another key challenge, as facility managers and service providers often need to monitor or update BEMS components remotely. To do so safely requires secure access channels, typically involving VPNs, multifactor authentication, and role-based permissions [14]. Systems must also support real-

doi:10.20944/preprints202505.0702.v1

time intrusion detection, continuously monitoring network traffic for anomalies that could indicate an attack. Resilience is equally critical, since BEMS should be capable of failing safely. For instance, reverting to a default operational mode if the AI layer or communication infrastructure is compromised. Implementing such fail-safes adds complexity but is essential for safety and compliance. The rise of demand-response–ready BEMS further expands the security perimeter. These systems must maintain secure bi-directional communication with the grid, making them potential entry points for attackers if not properly protected [2]. At the same time, maintaining strict local access control remains vital to protect internal building systems [31]. Retrofitting legacy systems poses additional risks and challenges. Many existing buildings include older equipment that lacks native support for modern security protocols. Updating or isolating these devices is often necessary but can be costly and logistically difficult [14]. Compounding the challenge is IoT lifecycle management, ensuring that all connected devices, which could number in hundreds or thousands, receive timely security patches. Devices that reach end-of-life and no longer receive updates must be isolated or removed to preserve the integrity of the overall system [14]. Some researchers advocate using AI to strengthen cybersecurity itself, such as through AI-based anomaly detection systems within BEMS networks. These can enhance real-time threat detection but also introduce new challenges related to explainability and trust in critical security contexts. As cybersecurity threats evolve, maintaining a compliant and resilient BEMS is a continuous effort requiring careful architectural decisions, secure component selection, and proactive operational practices.

Integration and Interoperability Challenges: As hinted earlier, interoperability is both a regulatory goal and a persistent technical challenge. Modern BEMS must often integrate multiple subsystems: HVAC controls using legacy protocols such as BACnet, Modbus [49], or KNX, lighting systems, security and access control, fire safety, and a wide array of IoT sensors from different vendors. Achieving seamless communication among these disparate components is complex and resource intensive. Engineers frequently rely on middleware platforms or protocol gateways that can translate between these heterogeneous systems. For example, a building might deploy an IoT integration layer that collects data from proprietary sensor networks and converts it into a standardized format for AI algorithms to analyze. While necessary, this architecture introduces latency and new points of failure, increasing system complexity and operational risk. Interoperability also involves connecting BEMS with external data sources such as electricity price signals from the grid, weather forecast APIs, or demand-response signals. This integration is vital for energy efficiency and grid interaction but requires robust handling of diverse data formats and secure external interfaces. Demand-response–ready systems must be capable of receiving standardized signals from grid operators while maintaining internal control integrity [12]. Furthermore, the EPBD's smart-readiness indicator and mandate for continuous monitoring and benchmarking [12] imply that BEMS must support standardized data export for national certification platforms and performance reporting. Meeting these obligations has encouraged the adoption of open metadata models like Project Haystack [50] and Brick Schema [51], though the building automation sector remains fragmented and inconsistent in implementation. From a compliance standpoint, buildings aiming to demonstrate smart-readiness or participate in energy flexibility markets must provide evidence that their BEMS can interoperate using accepted standards. This regulatory pressure is pushing vendors to adopt open protocols and interoperable system designs. However, legacy infrastructure presents a major barrier: many existing devices lack support for open standards and require either replacement or creative retrofitting. Bridging legacy protocols, such as BACnet, Modbus, or LonWorks, into unified control strategies remains one of the most cited and costly technical hurdles [2], [12]. One notable case study describes the difficulty of integrating "various devices and systems within a building" due to conflicting data semantics across BACnet, and Modbus systems [2]. Such efforts often extend deployment timelines and increase project costs but are critical for long-term compliance and system evolution. Harmonized HEMS/BEMS architectures that couple AI, IoT, and cybersecurity are already being tested in multi-country pilots to demonstrate how such interoperability can work in practice [52]. Enabling interoperability, however, can also introduce new cybersecurity vulnerabilities. Every additional interface increases the potential attack surface, necessitating robust access controls and secure authentication mechanisms at integration points. Engineers must strike a careful balance between openness and security to ensure both regulatory compliance and operational resilience. As smart building infrastructure becomes more interconnected, the ability to integrate securely and efficiently will define the viability of BEMS platforms in future energy systems.

Ensuring Performance Under Regulatory Constraints: A subtle but significant challenge in deploying AI-driven Building Energy Management Systems (BEMS) is ensuring high performance while complying with regulatory requirements. Compliance-related features, such as encryption, fine-grained access controls, and detailed logging, all introduce computational and architectural overhead that can impact system responsiveness and scalability. Moreover, AI algorithms must increasingly be tuned not solely for energy optimization but also to respect constraints related to occupant comfort, data privacy, and ethical boundaries. For instance, extreme energy-saving actions that compromise indoor climate might be seen as infringing on occupant rights or well-being. This has led to growing interest in multi-objective optimization strategies that balance energy efficiency, comfort, and privacy [53]. One example is a scenario where an AI system deliberately avoids exploiting a high-efficiency opportunity because doing so would require processing highly sensitive personal data, thus taking a privacy-aware but less efficient decision. Designing AI policies that can navigate such trade-offs is a complex challenge at the intersection of technology, ethics, and policy. Regulatory frameworks like the GDPR also affect how AI systems handle data. Restrictions on long-term storage of personal data can limit an AI model's ability to learn from historical behavioral trends. To address this, developers are experimenting with techniques such as on-device learning, abstract feature extraction, and federated learning [45], where the raw data never leaves the device, and only model updates are shared across systems. Differential privacy methods [54] are also being prototyped to ensure that learning processes do not compromise individual privacy. Still, enforcing data retention policies across diverse device types remains difficult, prompting interest in solutions like verifiable deletion frameworks, such as IoT Expunge, which aim to provide proof that data has been irreversibly removed when required [25]. Balancing performance, compliance, and ethical considerations is not a one-time design issue but an ongoing systems engineering task. It requires continuous tuning of AI models, careful selection of data-handling strategies, and deep integration of policy constraints into system architecture, all while maintaining the responsiveness and reliability expected of modern BEMS.

In summary, the technological challenges in deploying AI/IoT BEMS in the EU are tightly coupled with the regulatory demands. Solutions are emerging – like edge computing for privacy, XAI methods for transparency, "secure by design" architectures for cyber resilience, and open protocols for interoperability – but each comes with trade-offs. Addressing these challenges, likely requires interdisciplinary collaboration: computer scientists, control engineers, cybersecurity experts, and legal experts working together to ensure the next generation of BEMS can tick all the compliance boxes and deliver high performance. The effort is worthwhile, as the next section will discuss, because a compliant design unlocks various economic and strategic opportunities.

3.3. Economic Opportunities in Regulatory-Compliant Smart BEMS

Despite the hurdles, the intersection of AI/IoT and EU regulations in building management also opens up significant economic opportunities. By adhering to and leveraging these regulations, stakeholders can achieve cost savings, tap into new markets, and enhance the value proposition of smart building technologies. The review findings highlight several promising opportunities:

Energy Efficiency Gains and Cost Savings: The primary economic driver for AI-enabled BEMS is improved energy efficiency, which directly translates to cost savings on utility bills. Numerous case studies and field trials across Europe have demonstrated that intelligent control strategies can substantially reduce energy consumption in buildings, often by 15–30% or more on average [1]. Energy-efficiency gains documented for AI HVAC optimization translate directly into OPEX savings

[1], [55]. For instance, machine learning algorithms that predict and pre-heat or precool spaces based on occupancy patterns and weather forecasts ensure that energy is used only when and where needed, eliminating waste. These savings have a dual benefit under EU policy: they not only lower operational costs for building owners but also help comply with increasingly strict energy performance standards like those mandated by the EPBD for renovations and new buildings. In other words, investing in an AI-driven BEMS can be a way to meet regulatory energy targets and avoid penalties or fines for non-compliance with building codes. Moreover, improved energy efficiency can lead to indirect economic gains such as higher building asset value and more favorable green building certifications. Studies have shown that buildings equipped with advanced energy management systems achieve sustainability ratings e.g. LEED, BREEAM faster or at higher levels [56], which in turn can command premium rents or sale prices. Under upcoming carbon pricing and emission trading schemes, reducing energy use in buildings might also yield tradable credits or reduced carbon taxes effectively monetizing efficiency. Thus, regulatory-compliant BEMS ensuring, for instance, that GDPR doesn't impede data-driven efficiency measures enables building owners to capture these energy cost savings confidently and sustainably.

Demand Response and Grid Services Revenue: Another economic opportunity lies in the ability of smart buildings to provide flexibility services to the electricity grid. EU energy policy is moving towards a decentralized, smart grid paradigm where consumers or "prosumers" actively participate in demand-response programs to help balance the grid and integrate renewable energy. Buildings with AI-driven management can automatically adjust their loads HVAC, EV chargers, thermal storage, etc. in response to price signals or grid requests, essentially behaving like thermal energy storage or fast-response resources. By doing so, they can earn incentives or payments from utilities or grid operators for demand response [2], [38]. For example, a commercial building that lowers its cooling load during peak demand hours with minimal comfort impact due to prior pre-cooling orchestrated by AI might receive a payment or bill credit. These programs exist in many EU countries and are expected to grow as part of achieving the EU Green Deal objectives [57]. BEMS that are interoperable and compliant, e.g. able to receive standardized signals, and secure enough to be trusted in grid programs will be the ones positioned to capitalize on this. Some building owners are already aggregating multiple buildings to offer significant load reduction or even using onsite generation and storage in coordination with BEMS to sell energy or services back to the grid. This effectively creates a new revenue stream enabled by smart BEMS, turning energy flexibility into an asset. Regulations like the Electricity Market Directive [58] part of the EU Clean Energy Package [59] support this by requiring Member States to enable demand response participation and dynamic pricing, so the regulatory environment is favorable for buildings to monetize their flexibility.

Market Growth and Innovation Opportunities: At an industry level, the need for regulatory-compliant solutions is driving innovation and market growth. Companies that can offer "compliance-ready" BEMS products. For example, controllers with built-in GDPR-compliant data handling or AI software that is pre-certified under the AI Act are likely to gain a competitive edge. There is a growing market for consultancy and technology solutions that help navigate compliance privacy filters for building data, cybersecurity modules for legacy building systems, etc. In essence, regulations create new niches and a demand for specialized tech. One clear indicator is the smart building market projections in Europe, here the market size for smart building technologies in Europe was valued at around $5.3 billion in 2023 and is forecast to grow to nearly $18.6 billion by 2030, at a robust CAGR of about 19–20% [60]. This growth is attributed not only to falling sensor and computing costs but also to policy-driven demand, as EU directives like the EPBD are pushing building owners to invest in automation and smart controls, and in turn, vendors are racing to supply solutions that meet the new standards. Furthermore, by embracing EU's high standards early, companies can position themselves for the global market. The so-called "Brussels Effect" means EU regulations often set benchmarks adopted elsewhere [8]. For example, if a company develops an AI BEMS that complies with the strict EU AI Act and GDPR, it likely will meet or exceed requirements in other regions, giving it a first-mover advantage internationally. Early compliance also builds customer trust;

doi:10.20944/preprints202505.0702.v1

building owners have more confidence in solutions that are certified secure and privacy-friendly, which can shorten sales cycles and command higher prices. As Pery 2024 notes, "Compliance not only strengthens customer trust and brand reputation, but also positions companies to be ready for future regulations" [8]. This is an opportunity for European tech providers to become leaders in "trusted AI IoT" for smart buildings, a marketable quality as data security and privacy become top-of-mind for all clients.

Operational Savings and Facility Management Optimization: Beyond energy costs, AI/IoT BEMS can reduce other operational costs and even enable predictive maintenance, which has economic benefits. For example, machine learning can analyze equipment data to predict failures like an HVAC unit starting to degrade so maintenance can be done proactively, avoiding more costly breakdowns. This ties into regulations indirectly, as some EU regulations e.g. EPBD require regular inspections of systems like boilers and AC for efficiency. A smart BEMS that continuously monitors performance might eventually be allowed to replace or extend the interval of mandatory inspections [12], saving cost and time, if regulators trust the continuous commissioning capabilities. Moreover, improved occupant comfort and indoor environmental quality, by achievable with AI fine-tuning, can have productivity benefits in workplaces and health benefits, which, while harder to quantify, have economic value e.g. fewer sick days, higher employee satisfaction. Some building owners and investors are recognizing that smart, well-controlled buildings are future-proof against regulatory changes and climate-related risks, thus protecting their asset value. This is sometimes discussed under the banner of ESG investing, where buildings with good ESG profiles attract more investment.

Incentives and Funding Alignment: EU and national governments have also set up various incentive programs that effectively subsidize the adoption of compliant smart building technologies. For instance, as part of COVID-19 recovery funds and green transition funds, many countries offered grants or tax incentives for digital upgrades in buildings that improve energy performance. A BEMS that demonstrably saves energy and enhances grid responsiveness can qualify for such programs, reducing the upfront cost for the owner. Horizon Europe and other research funding initiatives have poured money into pilot projects and living labs for smart buildings where companies participating not only get funding but also shape standards. Regulatory sandboxes as mentioned earlier can provide both a relaxed regulatory environment and financial support to test innovative BEMS business models, for example, aggregating buildings in a local energy community. Participation in these programs is an opportunity to be at the cutting-edge and to form partnerships with utilities, tech firms, cities that can lead to new business opportunities.

In conclusion, while compliance with EU regulations requires effort, it unlocks significant economic upside. Energy and operational cost savings directly improve the bottom line for building operators. New revenue streams through grid services and market opportunities through offering compliant solutions expand the top line for innovative companies. Compliance itself is becoming a differentiator: consumers value security-labelled devices [10], and EESC opinions highlight growing public demand for privacy-preserving solutions [61], [62]. Although barriers such as cost, reliability, and privacy concerns continue to suppress adoption, particularly in the residential segment [63], initiatives like SMART2B demonstrate promising low intrusion retrofit pathways [39]. Crucially, by aligning technology development with policy goals, stakeholders ensure they are not just reacting to regulations but leveraging them as a catalyst for modernization and value creation. The European context, with its ambitious climate targets and digital agenda, essentially guarantees that smarter, greener buildings will be rewarded through savings, market preference, and often direct incentives.

4. Discussion

This scoping review has brought to light the intricate interplay between EU regulations and the adoption of AI/IoT in advanced BEMS. The findings illustrate a landscape of trade-offs and synergies that policymakers, technologists, and industry stakeholders must navigate. In this discussion, we synthesize the results, reflect on the implications for industry practice and policy, and identify areas where further research or policy experimentation is warranted.

Regulatory Push-Pull Dynamics: One of the overarching observations is that EU regulations simultaneously push and pull the adoption of smart building technologies. On one side, initiatives like the EPBD with its smart readiness emphasis and BACS mandate and energy market reforms actively push building owners to adopt AI/IoT solutions as a means to achieve energy targets and enable a flexible grid. On the other hand, horizontal regulations on data, AI, and security impose conditions that can slow down adoption if not properly addressed, creating a form of regulatory friction. This push-pull dynamic can be seen as a deliberate balancing act, where the EU encourages innovation but within a framework that safeguards public interest values privacy, safety, cybersecurity, etc. For the industry, this means innovation cannot occur in a vacuum, it must be responsible innovation. The discussion in the literature often pointed out that ignoring regulations is not an option in Europe; instead, success will come from innovating with compliance in mind from the ground up what some call a “compliance-by-design” or “ethics-by-design” approach to AI development [26], [17]. In practice, companies integrating AI/IoT into BEMS in the EU are developing multidisciplinary teams including legal compliance officers or data privacy experts alongside engineers early in product design. This contrasts with perhaps a more laissez-faire approach in other regions. The trade-off here is speed vs. sustainability: a heavily regulated environment might slow initial deployment, but it could lead to more robust, trustworthy solutions that have staying power and broader acceptance. Indeed, a theme that emerged is that regulation can be an enabler of trust, as building owners are more likely to adopt AI/IoT if they have assurance backed by law that their data will be protected, and the systems are safe. In that sense, the EU’s strict rules might actually improve adoption in the long run by overcoming end-user hesitancy.

Addressing the Compliance Burden: That said, there is an undeniable compliance burden that especially smaller tech companies or building operators face. For example, a startup developing an AI-based building control algorithm now has to worry about documentation and conformity assessment for the AI Act, something that might be resource-intensive. Similarly, a facilities management company deploying IoT sensors must implement GDPR processes data protection impact assessments, appointing a Data Protection Officer, etc. The review found calls for clearer guidance and tools to help navigate these requirements. This is where regulatory sandboxes and standardization efforts come into play [9], [48]. Regulatory sandboxes or controlled environments where companies can pilot innovations under the supervision of regulators are suggested as a way to test AI BEMS solutions with temporary relaxations or support [44]. For instance, a national authority might allow a hospital to pilot a new AI ventilation control system in a sandbox, monitoring its performance and compliance, and using those insights to refine both the product and the interpretation of regulations. The AI Act explicitly encourages Member States to set up such sandboxes, and the building sector could benefit from being included in these early trials. This collaborative approach can identify disproportionate burdens and inform more nuanced regulatory guidance or even adjustments. Another mechanism to ease compliance is the development of standards and certification schemes. If clear European or international standards emerge for, say, “Building AI Control System Safety” or “Privacy in Smart Buildings”, complying with those standards could be a presumptive way to meet regulatory requirements much like how ISO 27001 certification can demonstrate good cybersecurity practice. Industry coalitions and EU agencies are already working on frameworks. For example, CEN-CENELEC is likely to develop standards in support of the AI Act’s essential requirements. Adopting such standards could simplify the process for innovators, by giving them a checklist to follow and eliminating the need for examining every solution in an ad hoc manner. In summary, while the compliance burden is real, there are emerging strategies to streamline it, and the discussion emphasizes the importance of public-private collaboration in this space.

Implications for Building Industry Stakeholders: Different stakeholders in the building ecosystem will experience these regulatory impacts in distinct ways. Building owners and investors need to recognize that smart technologies are no longer optional frills but are becoming part of compliance and best practice. Ignoring AI/IoT could mean falling foul of efficiency mandates or missing out on incentives. However, owners also must be cognizant of the risks; for example, if they implement a sophisticated system, they inherit certain legal responsibilities data controller obligations under GDPR, etc. This is driving changes in procurement: tenders for building systems in the EU now often include requirements for GDPR compliance, cybersecurity features, and even alignment with upcoming AI rules. Technology providers and system integrators face the challenge of up-skilling in domains like cybersecurity and privacy. A BEMS vendor might need to hire privacy engineers or obtain security certifications to remain competitive. Those that do so effectively can market their solutions as “regulation-ready”, which, as noted, is becoming a selling point. For policy makers and regulators, the implication is that enforcement and guidance go hand in hand. There is a fine line between enforcing rules strictly to ensure compliance and not stifling innovation. The discussion in sources often highlighted the need for continuous dialogue: as new regulations like the AI Act roll out, regulators might need to issue sector-specific guidelines e.g. an EU guidance note on AI in energy management to clarify expectations in the building context. Similarly, data protection authorities DPAs could provide examples of GDPR-compliant smart building deployments to guide the industry. One concrete suggestion in the literature is developing regulatory harmonization between domains. For instance, ensuring the AI Act’s requirements dovetail with GDPR obligations so that an AI system that follows one isn’t inadvertently violating the other. An example would be clarifying how to handle personal data in AI training datasets for buildings, which the European Data Protection Board EDPB has started to do in recent opinions.

Future Research Directions: The scoping nature of this review means it identified broad areas but also gaps that future research should delve into. One key area is quantitative evidence of the impact of regulations on the adoption of advanced BEMS. While we qualitatively discussed barriers and opportunities, empirical studies could measure, for instance, how GDPR has affected deployment rates of occupancy sensors or how much the additional security measures add to BEMS project costs. Such data would help calibrate policy are the benefits of a regulation proportionate to any slowdown in efficiency improvements. Another research direction is developing and testing privacy-preserving and secure AI techniques specifically for buildings, e.g. evaluating federated learning or differential privacy in a BEMS context to see if they truly satisfy GDPR and what the trade-offs are in energy performance. Pilot projects in different EU countries with different building types and climates could provide case studies to refine the best practices. User-centric research is also important: How do occupants feel about AI controlling their environment? Does informing them transparency improve acceptance, and what level of control do they expect to retain? These human factors will influence how regulations are implemented on the ground for example, requiring explicit notices in smart buildings about AI systems in use, akin to CCTV notices. There’s also a forward-looking need to research regulatory harmonization beyond the EU. As buildings increasingly incorporate global IoT products and cloud services, alignment between EU rules and those elsewhere like U.S. NIST frameworks [64] or ISO standards would ease technical implementation. Researchers can contribute by mapping equivalences and suggesting mutual recognition where appropriate.

Policy Evolution: The discussion would be incomplete without acknowledging that regulations themselves are not static. The EU framework for AI and data is still evolving. The AI Act is expected around 2025, enforcement a couple years after; the Data Act in 2024–2025. The implementation phase of these laws will be critical. How Member States enact NIS2 or how DPAs enforce GDPR in IoT contexts could significantly shape the outcomes. There is an opportunity for policy experimentation. For example, some countries might create specific “smart building compliance hubs” that combine energy, data, and AI regulators to provide one-stop guidance. If successful, these could become models for others. The notion of “proportional regulation” came up, meaning that requirements might need tailoring to the scale of risk: a small apartment building’s BEMS shouldn’t face the exact same process as a nationwide smart grid AI. Policymakers may need to clarify thresholds and exemptions to avoid over-burdening low-risk scenarios while keeping high-risk ones in check.

In balancing all the above, one can see the emerging narrative: Europe is positioning itself to lead in sustainable, human-centric AI in buildings. This is a strategic choice. Rather than purely maximizing technological capability or purely enforcing precautions, the EU approach tries to do both by encourage advanced BEMS deployments, but under rules that ensure those deployments contribute to societal goals decarbonization, with respect for rights, etc. If successful, the pay-off is not just energy savings in buildings, but a model of "trusted smart buildings" that other regions might emulate. If too restrictive, there is a risk that innovation could shift elsewhere or that EU buildings lag in tech adoption. The coming years will be a test of this balance.

5. Conclusions

This scoping review examined how EU regulations affect the adoption of AI and IoT technologies in advanced BEMS. We explored legal barriers, technical challenges, and economic opportunities, drawing on a wide range of sources from policy documents to engineering case studies. Several key takeaways emerged:

Legal Takeaways: The EU has put forth a comprehensive regulatory framework, including the GDPR for data privacy, the proposed AI Act for AI governance, the Cybersecurity Act and NIS2 for security, and the EPBD for building performance, that collectively directly influences smart building deployments. These regulations create obligations such as ensuring data transparency, securing devices and networks, and providing human oversight of AI decisions. Compliance with these rules is now a core requirement for any AI/IoT solution in European buildings. While they pose challenges, like needing to implement privacy-by-design, maintain extensive documentation, and undergo security audits, they also provide clear guidelines that can improve the trust and reliability of BEMS. In short, EU laws act as guardrails to ensure that as buildings get "smarter", they also get safer, more secure, and more respectful of occupant rights.

Technological Takeaways: Designing a regulatory-compliant BEMS demands interdisciplinary technical solutions. Key challenges include managing data locally or anonymizing it to satisfy privacy concerns, developing explainable AI so that automated decisions can be understood and justified, hardening systems against cyber threats, and integrating a plethora of devices and protocols to meet interoperability goals. The state-of-the-art is evolving with new algorithms that allow federated learning across buildings, and standard data models are easing integration, but gaps still remain. Importantly, many compliance-related features like encryption, logging, and consent management interfaces must be built-in from the start. The review highlighted that "smart" must go hand-in-hand with "secure and transparent" in the next generation of BEMS. Technologists are rising to this challenge by innovating in areas like secure IoT hardware, AI explainability tools, and privacy-preserving analytics specific to smart buildings.

Economic Takeaways: Far from stifling the market, EU regulations in many cases are spurring innovation and growth in smart building technologies. Buildings equipped with AI and IoT that operate within the regulatory guardrails stand to reap significant economic benefits: reduced energy and maintenance costs, payments for grid support services, and higher asset values. We are seeing a maturing market where compliance capabilities are a competitive differentiator. For example, a smart thermostat that is GDPR-compliant and cyber-secure may be preferred by consumers and mandated in public tenders. The European smart buildings market is forecast to expand rapidly over the coming decade, indicating strong investment momentum. Regulations like the EPBD ensure that this growth contributes to climate goals e.g. cutting emissions and peak demand. Moreover, by adhering to high standards, European solutions are gaining an edge globally as demand for trusted smart building solutions rises worldwide. In essence, when done right, regulatory compliance becomes an opportunity: it drives quality improvements that open new business models and markets, from energy flexibility services to premium "smart building" certifications and beyond.

The adoption of AI and IoT in BEMS within the EU is a story of synergy between technology and policy. The regulations in place form a robust framework that, while challenging, ensures that the digital transformation of buildings aligns with societal values and energy transition goals. Rather than viewing these rules as roadblocks, forward-looking companies and building operators are treating them as a checklist for innovation that inspire new technical solutions and give confidence to scale up smart building deployments. To fully realize the vision of intelligent, efficient, and user-centric buildings, stakeholders must continue this collaborative path: regulators remain receptive to feedback and adapting rules as needed, and industry embracing a compliance-by-design mentality.

Finally, we note that this is an evolving domain. Continuous monitoring of policy implementation and outcomes is recommended. Future research and pilot projects, especially those in living labs or regulatory sandboxes, will be invaluable to refine best practices. Questions such as how to quantify the ROI of compliance measures, or how occupants perceive AI in buildings under different transparency approaches, merit further investigation. Nonetheless, the trajectory is clear: regulatory-compliant AI/IoT solutions in BEMS are not only feasible, but they represent the future of sustainable smart buildings in Europe, buildings that intelligently manage energy, keep occupants comfortable and safe, and do so in a way that upholds the European ideals of privacy, security, and accountability. By navigating the challenges and seizing the opportunities, stakeholders can ensure that our buildings become both smarter and better, contributing meaningfully to a greener and more digital Europe.

Author Contributions: Both authors have contributed equally to the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
AI Act	Artificial Intelligence Act (EU)
AIA	Artificial Intelligence Act (alternate abbreviation used once)
AI/IoT	Artificial Intelligence / Internet of Things
AILD	AI Liability Directive
API	Application Programming Interface
BACnet	Building Automation and Control network
BACS	Building Automation and Control Systems
BAS	Building Automation System
BEMS	Building Energy Management System
CAGR	Compound Annual Growth Rate
CEN-CENELEC	European Committee for Standardization – European Committee for Electrotechnical Standardization
DPAs	Data Protection Authorities
EDPB	European Data Protection Board
ENISA	European Union Agency for Cybersecurity
EPBD	Energy Performance of Buildings Directive
ESG	Environmental, Social, Governance
EU	European Union
EV	Electric Vehicle
GDPR	General Data Protection Regulation
HEMS	Home Energy Management System
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and Communication Technology
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
KNX	A standardized communication protocol for building automation
LEED	Leadership in Energy and Environmental Design
ML	Machine Learning
Modbus	A communication protocol for building and industrial automation systems
NIS	Network and Information Security Directive
NIS2	Revised Network and Information Security Directive

OPEX	Operating Expenditure
OT	Operational Technology
PLD	Product Liability Directive
PRISMA-ScR	Preferred Reporting Items for Systematic Reviews and Meta-Analyses – Scoping Review
SRI	Smart Readiness Indicator
VPN	Virtual Private Network
WoS	Web of Science
XAI	Explainable Artificial Intelligence

References

1. D. M. T. E. Ali, V. Motuzienė, and R. Džiugaitė-Tumėnienė, "AI-Driven Innovations in Building Energy Management Systems: A Review of Potential Applications and Energy Savings," *Energies,* vol. 17, no. 17, p. 4277, 2024/08/27 2024, doi: 10.3390/en17174277.
2. B. M. S. Controls, "BEMS for Smart Grid Integration and Demand Response," 2023 2023. [Online]. Available: https://bmscontrols.co.uk/blog/bems-for-smart-grid-integration-and-demand-response/.
3. U. P. Build, "Overview Article - Smart Buildings and Smart Technologies in Europe: State of Play and Perspectives," BUILD UP, Brussels, 2021/07/15 2021. [Online]. Available: https://build-up.ec.europa.eu/en/resources-and-tools/articles/overview-article-smart-buildings-and-smart-technologies-europe-state
4. C. European, "Advancing the Internet of Things in Europe," European Commission, Brussels, 2016/04/19 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110
5. C. European, "Interoperable and Smart Homes and Grids (H2020_DT-ICT-10-2018-19)," European Commission, Brussels, 2018/10/27 2018. [Online]. Available: https://cordis.europa.eu/programme/id/H2020_DT-ICT-10-2018-19
6. A. Abu Bakar, S. Yussof, A. Abdul Ghapar, S. S. Sameon, and B. N. Jørgensen, "A Review of Privacy Concerns in Energy-Efficient Smart Buildings: Risks, Rights, and Regulations," *Energies,* vol. 17, no. 5, p. 977, 2024/02/20 2024, doi: 10.3390/en17050977.
7. *Regulation (EU) 2024/1689 - Artificial Intelligence Act*, COM/2021/206 final, 2021.
8. A. Pery, "How can IoT device manufacturers prepare for the EU AI Act?," 2024/12/02 2024. [Online]. Available: https://www.iotinsider.com/iot-insights/industry-insights/how-can-iot-device-manufacturers-prepare-for-the-eu-ai-act/.
9. *Regulation (EU) 2019/881 - Cybersecurity Act*, E. Union, 2019.
10. G. Thales, "IoT Cybersecurity: Regulating the Internet of Things – EU, US and UK Regulations 2024," Thales Digital Identity & Security, 2024/01 2024. Accessed: 2025/03/15. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations
11. *Regulation (EU) - Cyber Resilience Act*, 2024.
12. B. S. Muench, "Primer on the European Commission's Energy Performance of Buildings Directive (EPBD)," 2025/01/30 2025. [Online]. Available: https://www.j2inn.com/blog/primer-on-the-european-commissions-energy-performance-of-buildings-directive-epbd.
13. *Directive (EU) 2022/2555—NIS2 Directive*, 2023.
14. S. Veridify, "EU NIS2 Directive and Implications for BAS/BMS Cybersecurity," 2023 2023. [Online]. Available: https://www.veridify.com/eu-nis2-directive-and-implications-for-bas-bms-cybersecurity/.
15. *Regulation (EU) 2023/2854 - Data Act*, 2023.
16. C. European, "Sector inquiry into consumer Internet of Things," European Commission, Brussels, 2022/01/20 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0019
17. TrustArc, "European Union Data Privacy: What's Next for 2025?," 2023 2023. [Online]. Available: https://trustarc.com/resource/european-union-data-privacy-whats-next-for-2025/.
18. Prisma, "PRISMA Extension for Scoping Reviews (PRISMA-ScR)," 2024. [Online]. Available: https://www.prisma-statement.org/scoping.
19. *Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)*, 2016.

20. M. Mateev, "Iot, smart energy systems, personal data and encryption in the gdpr," 2017-01-01 2017, vol. 17, 2017, pp. 921-928, doi: 10.5593/sgem2017H/63/S27.114. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85063106733&origin=inward
21. T. Heino, S. Rauti, and R. Carlsson, "An assessment of privacy policies for smart home devices," 2023-06-16 2023, 2023, pp. 129-133, doi: 10.1145/3606305.3606332. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85179882005&origin=inward
22. C. I. Wickramasinghe, "Best-Practice-Based Framework for User-Centric Privacy-Preserving Solutions in Smart Home Environments," 2023, 2023. [Online]. Available: https://www.webofscience.com/wos/woscc/full-record/WOS:001316133900006.
23. C. I. Wickramasinghe and D. Reinhardt, "A User-Centric Privacy-Preserving Approach to Control Data Collection," 2022, 2022. [Online]. Available: https://www.webofscience.com/wos/woscc/full-record/WOS:000771894700011.
24. Z. Wu, A. B. Williams, and D. Perouli, "Dependable Public Ledger for Policy Compliance," 2019, 2019. [Online]. Available: https://www.webofscience.com/wos/woscc/full-record/WOS:000565234200176.
25. N. Panwar, S. Sharma, P. Gupta, D. Ghosh, S. Mehrotra, and N. Venkatasubramanian, "IoT Expunge: Implementing Verifiable Retention of IoT Data," 2020, 2020. [Online]. Available: https://www.webofscience.com/wos/woscc/full-record/WOS:001239371500036.
26. S. Pelekis *et al.*, "Trustworthy artificial intelligence in the energy sector: Landscape analysis and evaluation framework," 2024, 2024. [Online]. Available: https://www.webofscience.com/wos/woscc/full-record/WOS:001429193000010.
27. C. European Union Agency for, "Security and Resilience of Smart Home Environments," ENISA, Brussels, 2015/12/01 2015. [Online]. Available: https://www.enisa.europa.eu/publications/security-resilience-good-practices
28. N. European Union Agency for and S. Information, "Threat Landscape and Good Practice Guide for Smart Home and Converged Media," ENISA, Heraklion, Greece, 2014/12/01 2014. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/Threat%20Landscape%20and%20Good%20Practice%20Guide%20for%20Smart%20Home%20and%20Converged%20Media.pdf
29. Cordis, "Are smart buildings safe from hackers and privacy breaches?," European Commission, Brussels, 2017/03/01 2017. [Online]. Available: https://cordis.europa.eu/article/id/133295-are-smart-buildings-safe-from-hackers-and-privacy-breaches
30. D. Preuveneers and W. Joosen, "Security and privacy controls for streaming data in extended intelligent environments," *JOURNAL OF AMBIENT INTELLIGENCE AND SMART ENVIRONMENTS,* vol. 8, no. 4, pp. 467-483, 2016 2016, doi: 10.3233/ais-160384.
31. J. Bauer *et al.*, "ForeSight - An AI-driven Smart Living Platform, Approach to Add Access Control to openHAB," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12157 LNCS, (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), no. 12157 LNCS), 2020, pp. 432-440.
32. P. Gonzalez-Gil, R. Marin-Perez, A. González-Vidal, A. P. Ramallo-González, and A. F. Skarmeta, "Interoperable and Intelligent Architecture for Smart Buildings," 2021-01-01 2021: IEEE, 2021, pp. 359-364, doi: 10.1109/SmartIoT52359.2021.00067. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85125769460&origin=inward
33. B. Delinchant and J. Ferrari, *Standards and technologies from building sector, IoT, and open-source trends* (Towards Energy Smart Homes: Algorithms, Technologies, and Applications). 2021, p. 63.
34. B. U. E. Team, "What makes a building 'smart': technologies driving energy efficiency," BUILD UP – The European Portal For Energy Efficiency in Buildings, Brussels, 2025/03/05 2025. [Online]. Available: https://build-up.ec.europa.eu/en/resources-and-tools/articles/what-makes-building-smart-technologies-driving-energy-efficiency
35. B. A. Committee, "About the BACnet Standard," *BACnet Committee,* 2025/05/06/ 2025. [Online]. Available: https://bacnet.org/about-bacnet-standard/.

36. K. N. X. Association, "A brief introduction to KNX," 2025/05/06 2025. [Online]. Available: https://www.knx.org/knx-en/for-professionals/What-is-KNX/A-brief-introduction/.
37. A. D. R. A. Open, "OpenADR Alliance," *OpenADR Alliance,* 2025/05/06 2025. [Online]. Available: https://www.openadr.org/.
38. C. European, "Digitalising the energy system – EU action plan," European Commission, Strasbourg, 2022/10/18 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022SC0341
39. C. C. f. N. E. T. SA, "SMART2B – Smartness to Existing Buildings," European Commission, Brussels, 2021/09/01 2021. [Online]. Available: https://cordis.europa.eu/project/id/101023666
40. C. European, "Liability for Emerging Digital Technologies," European Commission, Brussels, 2018/04/25 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0137
41. S. De Luca, "Revised Product Liability Directive," European Parliamentary Research Service, Brussels, 2025/02 2025. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf
42. C. European, "Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)," 2022-09-28 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496
43. F. Norton Rose, "Artificial Intelligence and Liability: Key Takeaways from Recent EU Legislative Initiatives," 2024/07 2024. [Online]. Available: https://www.nortonrosefulbright.com/en-nl/knowledge/publications/7052eff6/artificial-intelligence-and-liability.
44. U. European, "Article 57: AI Regulatory Sandboxes | EU Artificial Intelligence Act," 2025 2025. [Online]. Available: https://artificialintelligenceact.eu/article/57/.
45. P. Swabey, "Why edge computing is a double-edged sword for privacy," ed, 2022.
46. A. Metwaly, J. P. Queralta, V. K. Sarker, T. N. Gia, O. Nasir, and T. Westerlund, "Edge computing with embedded AI: Thermal image analysis for occupancy estimation in intelligent buildings," 2019-10-13 2019, 2019, pp. 1-6, doi: 10.1145/3372394.3372397. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85079090531&origin=inward
47. P. Gailhofer, A. Herold, P. D. f. E. S. European Parliament, and P. Quality of Life, "The Role of Artificial Intelligence in the European Green Deal," European Parliament, Luxembourg, 2021/06/01 2021. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662906/IPOL_STU(2021)662906_EN.pdf
48. D. Technology Law, "ENISA Releases Comprehensive Framework for Ensuring Cybersecurity in the Lifecycle of AI Systems," ed: Technology Law Dispatch, 2023.
49. O. Modbus, "Modbus Specifications and Implementation Guides," 2025/05/06 2025. [Online]. Available: https://www.modbus.org/specs.php.
50. O. Project Haystack, "Project Haystack," *Project Haystack,* 2025/05/06. [Online]. Available: https://www.project-haystack.org/.
51. *Brick Schema: A Uniform Metadata Schema for Buildings*, T. B. Consortium, 2025. [Online]. Available: https://brickschema.org/
52. C. European, "Progress on competitiveness of clean energy technologies," European Commission, Brussels, 2021/10/26 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021SC0307
53. S. Lee, L. Xie, and D.-H. Choi, "Privacy-Preserving Energy Management of a Shared Energy Storage System for Smart Buildings: A Federated Deep Reinforcement Learning Approach," *Sensors,* vol. 21, no. 14, 2021, doi: 10.3390/s21144898.
54. J. K, B. H, T. H, and M. A. P, "A review of preserving privacy in data collected from buildings with differential privacy," *Journal of Building Engineering,* vol. 56, p. 104724, 2022/09/15/ 2022, doi: https://doi.org/10.1016/j.jobe.2022.104724.
55. M. W. Ahmad, M. Mourshed, D. Mundow, M. Sisinni, and Y. Rezgui, "Building energy metering and environmental monitoring - A state-of-the-art review and directions for future research," *ENERGY AND BUILDINGS,* vol. 120, pp. 85-102, 2016-05-15 2016, doi: 10.1016/j.enbuild.2016.03.059.

56. Dannie, "AI-Powered Building Energy Systems Cut Costs by 30% While Boosting Efficiency," *Industrial Build News*, 02/20
2025/02/20 2025. [Online]. Available: https://www.build-news.com/energy-management-and-efficiency/energy-management-systems/ai-powered-building-energy-systems-cut-costs-by-30-while-boosting-efficiency/.
57. (2019). *The European Green Deal*. [Online] Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en
58. (2025). *Electricity Market Design*. [Online] Available: https://energy.ec.europa.eu/topics/markets-and-consumers/electricity-market-design_en
59. C. European, "Clean Energy for All Europeans Package," 2019/05/22 2019. [Online]. Available: https://wayback.archive-it.org/12090/20241209144917/https://energy.ec.europa.eu/topics/energy-strategy/clean-energy-all-europeans-package_en.
60. I. Fortune Business, "Europe Smart Building Market Size, Share & Forecast 2030," Fortune Business Insights, 2023 2023. Accessed: 2025/03/10. [Online]. Available: https://www.fortunebusinessinsights.com/europe-smart-building-market-105128
61. E. European and C. Social, "The digital revolution in view of citizens' needs and rights," Official Journal of the European Union, Brussels, 2019/06/05 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018IE4168
62. E. European and C. Social, "Balancing opportunities and risks for European consumers (2024/C 134/16)," Official Journal of the European Union, Brussels, 2024/04/12 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024IE1212
63. P. C. K. Gamage, M. Haddara, and M. Langseth, "Uncovering the IoT Roadblocks: Exploring Barriers to Smart Home Adoption in Europe," in *Lecture Notes in Networks and Systems*, vol. 834, (Lecture Notes in Networks and Systems, no. 834), 2024, pp. 245-262.
64. E. Tabassi, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2023/01/26 2023. [Online]. Available: https://doi.org/10.6028/NIST.AI.100-1

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.