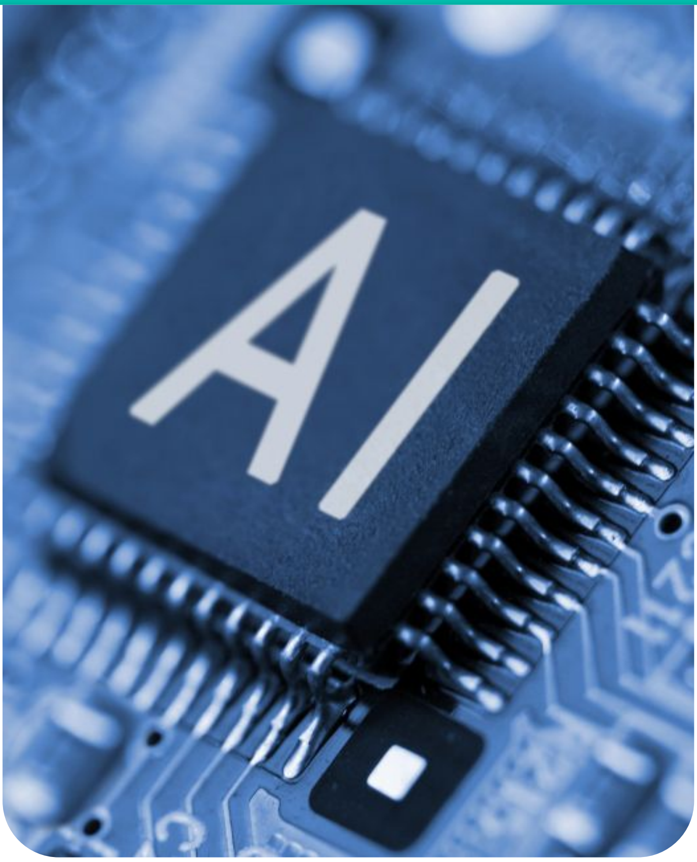
Compliance & Risks



From Smart Homes to Smart Laws: AI in Connected Products in the EU & US

Authors:
Dila Şen, Global Regulatory and Requirements Compliance Specialist, Compliance & Risks

Chelsea Cunningham, Senior Regulatory Compliance Specialist, Compliance & Risks

26 March, 2025

Further regulatory developments may have occurred after publication. To keep up-to-date with the latest compliance news, sign up to our newsletter

→ | complianceandrisks.com

Table of Contents

From Smart Homes to Smart Laws: AI in Connected Products in the EU & US

Table of Contents

From Smart Homes to Smart Laws: AI in Connected Products in the EU & US

01. About The Authors

Dila Şen,
Global Regulatory & Requirements Compliance Specialist,
Compliance & Risks

Dila Şen is a Turkish-qualified lawyer and sworn translator for 15 years with extensive experience in AI policy. She has been working as a Global Regulatory & Requirements Compliance Specialist at Compliance & Risks for five years.

Prior to joining Compliance & Risks, Dila worked for global companies like Lehman Brothers Holdings Inc., ADP, and several different law firms in Turkey as a legal counsel for several years.

Dila holds a triple LL.M. in European Master in Law & Economics from the Universities of Bologna, Ghent, and Haifa, and an LL.B. from Yeditepe University, where she was awarded a full merit-based scholarship by the Turkish government. She also holds a B.A. in Communication. She further developed her expertise in AI through an Advanced Certification from the Center for Artificial Intelligence & Digital Policy (CAIDP) in Washington, D.C., subsequently becoming a Team Leader. Currently, she is an AI Policy Group Member at CAIDP's AI Policy Clinic and an active member of the Istanbul Bar Association's AI Working Group.

Chelsea Cunningham,
Senior Regulatory Compliance Specialist,
Compliance & Risks

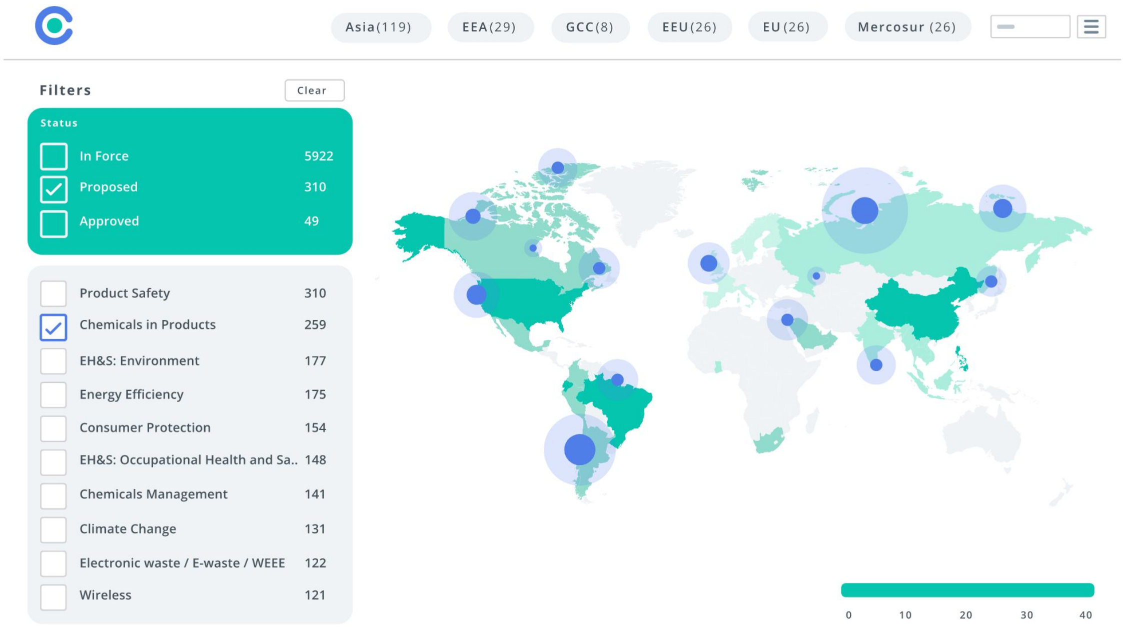
Chelsea is a highly experienced Senior Regulatory Compliance Specialist at Compliance & Risks, specializing in the electronics sector.

Her expertise spans global environmental, social and product safety regulations, and she leads the firm's Knowledge Partner Network, facilitating expert insights on product compliance.

With a strong academic background, including a MSc International Public Policy & Diplomacy, BCL and advanced AI certification, Chelsea brings a unique blend of regulatory, technological, and business acumen.

02. Unlocking Market Access

At Compliance & Risks, we help you keep on top of global regulatory changes and their impact worldwide. We have the right technology, regulatory content and expertise to help you unlock market access, protect revenue and elevate the role of compliance.



Asia(119) EEA(29) GCC(8) EEU(26) EU(26) Mercosur (26)

Filters Clear

Status

☐ In Force	5922
☑ Proposed	310
☐ Approved	49

☐ Product Safety	310
☑ Chemicals in Products	259
☐ EH&S: Environment	177
☐ Energy Efficiency	175
☐ Consumer Protection	154
☐ EH&S: Occupational Health and Sa..	148
☐ Chemicals Management	141
☐ Climate Change	131
☐ Electronic waste / E-waste / WEEE	122
☐ Wireless	121

Our solution includes:

- **C2P:** The most advanced product compliance and ESG compliance software on the market, helping you streamline your compliance process and unlock market access around the world.
- **Regulatory Content:** We provide the broadest and most comprehensive product compliance regulatory content on the market, monitoring 195+ countries, 20 industry sectors, 45 topics and 100,000+ regulatory sources.
- **Ask our Experts:** Direct access to our team of experts for support

Additionally, we offer:

✓ **Market Access Services:** Our Market Access team helps you understand your product compliance obligations by transforming regulations into actionable knowledge with tailored advice for you and your business.

Why choose C2P?

✓ **Stay ahead** of regulatory changes with the world's most comprehensive regulatory database

✓ **Avoid delays** with alerts of changes to regulations & requirements in real time

✓ **Improve efficiency with powerful collaboration and workflow tools** to keep compliance evidence up-to-date & live linked back to Regulations, Standards & Requirements

Contact us to speak to one of our team today to learn how you can simplify your regulatory compliance process.

For more information, please visit http://www.complianceandrisks.com

Important Notice: All information provided by Compliance & Risks Limited and its contributing researchers in this report is provided for strategic and informational purposes only and should not be construed as company-specific legal compliance advice or counsel. Compliance & Risks Limited makes no representation whatsoever about the suitability of the information and services contained herein for resolving any question of law. Compliance & Risks Limited does not provide any legal services.

03. Executive Summary: Navigating the Intersection of AI and Connected Products in the EU & US Legal Landscapes

The advancement of Artificial Intelligence (AI) within connected products is rapidly transforming industries across the European Union (EU) and the US, offering enhanced functionalities and unprecedented levels of automation.

From smart home devices and industrial machinery to connected vehicles and medical equipment, AI is increasingly embedded to improve performance, personalize user experiences, and drive innovation.

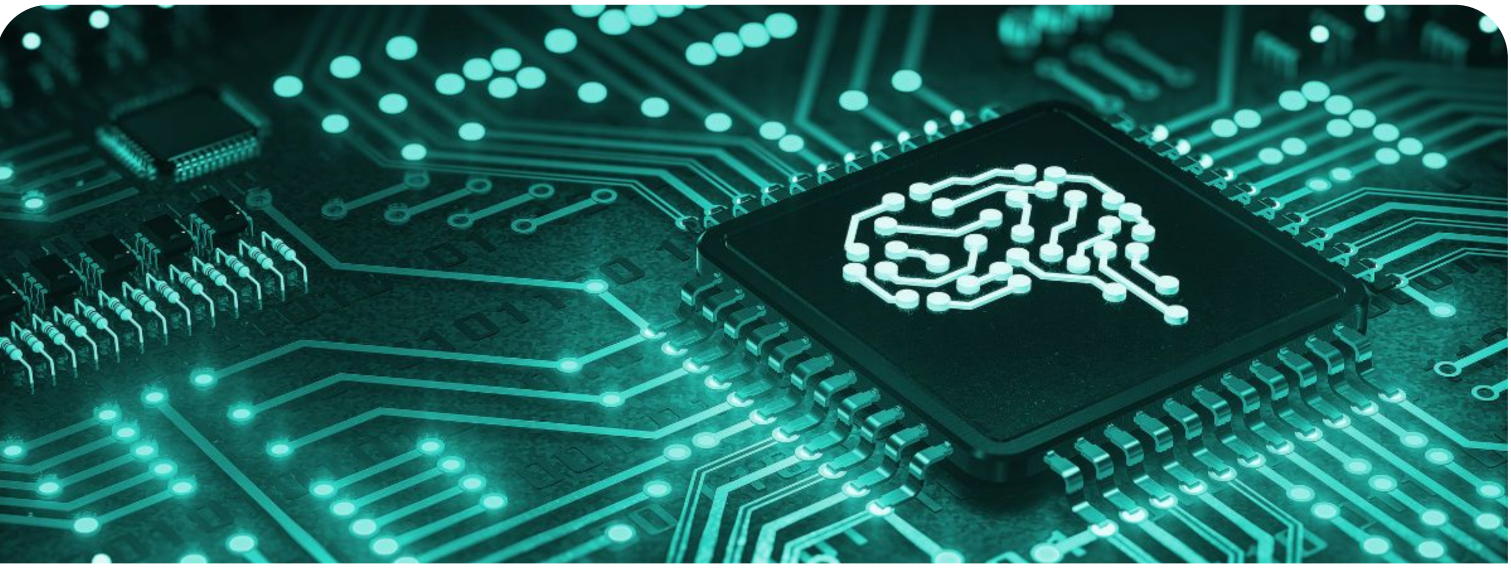
This surge in AI-powered connected products has coincided with the development of a comprehensive and evolving regulatory framework within the EU, designed to address the unique challenges and risks presented by these technologies. This framework encompasses not only sector-specific regulations but also horizontal legislation such as the EU Artificial Intelligence Act (AI Act), the Data Act, the General Data Protection Regulation (GDPR), and the Cybersecurity Act, creating a complex web of compliance obligations for businesses operating in this space.

In the US, regulation in this area is dynamic, with ongoing discussions and potential for new legislation, particularly in the ongoing Trump Administration. Similar to the EU, there is a growing emphasis on "security by design" meaning that security should be built into connected products from the initial development stage with various states introducing their own laws focusing on a number of key areas including, but not limited to; personal data protection, IoT, cybersecurity and AI, to name a few.

This whitepaper aims to provide a comprehensive analysis of the legal and regulatory landscape governing AI in connected products within the European Union and the US. It draws upon legal expertise and AI-driven analysis to offer an up-to-date perspective on the key definitions, principles, and requirements outlined in relevant legislation.

The objective is to equip companies with a clear understanding of their legal responsibilities and the strategic considerations necessary to navigate this evolving environment.

The integration of AI into connected devices necessitates a proactive and informed approach to legal compliance, as the regulatory landscape is still maturing. Companies must understand that compliance is not a singular effort but an ongoing process requiring continuous monitoring and adaptation to new guidance and enforcement priorities.



04. Defining the Scope: Understanding "AI" and "Connected Products" in the EU Context

4.1. Defining "AI System" under the EU AI Act

The cornerstone of the EU's regulatory approach to artificial intelligence is the definition of an "**AI system**" as laid out in Regulation (EU) 2024/1689, commonly known as the AI Act. Article 3(1) of this regulation defines an AI system as "*a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions, which can influence physical or virtual environments*".

Recital 12 further elaborates on this definition, highlighting the key characteristics of such systems, including their machine-based nature, their capacity to infer outputs based on received inputs, and their potential to impact the surrounding environment. This definition underscores the ability of AI systems to learn and adapt, operating with varying degrees of autonomy to achieve specific goals.

It is important to note that the AI Act generally excludes systems based solely on pre-programmed rules that do not involve inference or learning from data. The broad definition of "AI system" under the AI Act means that many functionalities within connected products, even seemingly simple ones, could potentially fall under its purview if they involve inference and learning. Recital 12 emphasizes the ability of AI systems to infer, learn, and adapt, suggesting a wide application to various technologies within connected products.

4.2. Defining "Connected Products" under EU Law

Complementing the AI Act is the definition of "**connected products**" provided by Regulation (EU) 2023/2854, known as the Data Act. Article 2(5) of the Data Act defines a "connected product" as "*an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access*". This definition encompasses a wide range of items capable of generating data about their operation or surroundings and transmitting this data through various means, including wireless or wired connections.

Examples of connected products are diverse, ranging from smart home appliances like refrigerators and thermostats to industrial machinery, medical devices such as health monitoring wearables, and consumer electronics like smartphones and televisions. It is crucial to distinguish these from products whose primary function is data storage, processing, or transmission, such as servers and routers, which are generally outside the scope of the Data Act unless they are owned, rented, or leased by the user. The Data Act provides a wide definition of "*connected products,*" encompassing a vast array of devices that generate data, highlighting the broad applicability of this regulation alongside the AI Act.

The interplay between the AI Act and the Data Act is crucial. A product can be "*connected*" under the Data Act and also incorporate an "*AI system*" under the AI Act, triggering obligations under both regulations. Both regulations address different aspects of technology in the EU market, with the AI Act focusing on the risks of AI and the Data Act on data access and use from connected products.

05. The EU Artificial Intelligence Act: Implications for Connected Products

5.1. Risk-Based Approach and Connected Products

The EU AI Act adopts a risk-based approach to the regulation of AI systems, categorizing them into four distinct levels of risk: unacceptable, high, limited, and minimal. This framework dictates the level of regulatory scrutiny and the obligations imposed on providers and deployers of AI systems. Determining how AI used in connected products might be classified under this framework requires careful consideration of the product's intended purpose and its potential impact on health, safety, and fundamental rights.

Annex III of the AI Act provides a list of high-risk AI systems, and certain AI-powered connected products have the potential to fall within these categories. Notably, connected products incorporating AI as a safety component in sectors already subject to EU harmonization legislation, as listed in Annex I of the AI Act, are automatically classified as high-risk. Examples of such products include AI-enabled medical devices, which are subject to the Medical Devices Regulation, and AI used in the safety systems of vehicles, which fall under relevant automotive safety regulations.

Furthermore, even if the AI in a connected product is not directly a safety component, its use in areas listed in Annex III, such as education, employment, essential private and public services, law enforcement, and the management and operation of critical infrastructure, could also lead to a high-risk classification. Annex III lists the high-risk AI applications based on their intended purpose. For instance, AI-powered connected devices used for remote patient monitoring or for managing critical infrastructure like energy grids would likely be considered high-risk due to their potential impact on health and safety.

5.2. Key Articles and Recitals Relevant to AI in Connected Products

5.2.1. Risk Classification (Articles 6, 9, Annex III)

Article 6 of the AI Act lays down the classification rules for high-risk AI systems, providing the criteria for determining which AI systems, including those embedded in connected products, fall under this higher level of regulation. Providers of high-risk AI-powered connected products are obligated under Article 9 to establish and maintain a robust risk management system. This system must encompass a continuous iterative process throughout the entire lifecycle of the AI system, requiring the identification of foreseeable risks, the implementation of risk mitigation measures, and the monitoring of residual risks. The requirement for a risk management system under Article 9 necessitates a comprehensive process for identifying, assessing, and mitigating risks associated with AI in connected products throughout their lifecycle.

Annex III further specifies the categories of high-risk AI systems based on their intended purpose, and careful consideration is needed to assess whether the functionalities of AI in connected products align with any of these categories, such as those used in safety components of regulated products or in critical infrastructure.

Recitals 19, 31, 49, and 51 provide important context, clarifying the rationale behind classifying certain AI systems as high-risk due to their potential to cause harm, violate fundamental rights, or impact the safety of products already subject to other EU regulations.

5.2.2. Transparency Obligations (Articles 13, 50)

Transparency is a core principle of the AI Act, and Articles 13 and 50 outline specific obligations for providers and deployers of AI systems, including those in connected products.

Article 13 mandates that providers of high-risk AI-powered connected products ensure transparency and provide comprehensive information to those who will deploy these products. This information must include the capabilities and limitations of the AI system, its expected performance, and any known risks or potential impacts. Article 50 lays out broader transparency obligations for various types of AI systems, particularly those intended to interact with natural persons, be used to generate or manipulate content, or generate synthetic content. This includes a crucial obligation to inform users that they are interacting with an AI system unless it is obvious from the context.

Transparency obligations under Articles 13 and 50 require clear and accessible information for both deployers (e.g., businesses using the connected product) and end-users about the AI system's capabilities, limitations, and how it processes data. These articles highlight the need to inform users about interacting with AI and provide the necessary information to ensure they can make informed decisions. Recitals 6, 72, and 171 underscore the significance of transparency in fostering trust in AI systems and ensuring accountability for their use.

For connected products with AI that interact directly with users, such as smart assistants or AI-powered chatbots within a device interface, the requirements of Article 50 are particularly relevant, necessitating clear disclosures about the AI's presence and functionalities.

5.2.3. Conformity Assessment (Article 43)

Before being placed on the market or put into service in the EU, high-risk AI-powered connected products must undergo a relevant conformity assessment procedure as outlined in Article 43 of the AI Act. This process is designed to ensure that the AI system meets the stringent requirements set forth in the Regulation. For many connected products that already fall under other EU regulations, such as medical devices or toys, the conformity assessment will often involve a third-party notified body. Conformity assessment, especially for high-risk AI in connected products, will likely involve demonstrating compliance with various technical and organizational requirements, potentially requiring significant investment and process adjustments for manufacturers. The conformity assessment and the classification of high-risk AI imply a rigorous evaluation process that may include the examination of technical documentation, testing of the AI system, and audits of the provider's quality management system. Recital 78 provides the rationale for these assessments, emphasizing their role in ensuring that high-risk AI systems comply with the AI Act's requirements and thereby protect health, safety, and fundamental rights. Upon successful completion of the conformity assessment, the provider must draw up an EU declaration of conformity and affix the CE marking to the product, indicating compliance with the AI Act.

5.2.4. Obligations of Providers and Deployers (Articles 16, 26)

Articles 16 and 26 of the AI Act delineate the specific obligations of providers and deployers of high-risk AI-powered connected products, respectively. Article 16 outlines a comprehensive set of responsibilities for providers, including ensuring that their high-risk AI systems comply with all relevant requirements of the Act. Providers must also indicate their name and contact information on the product or its packaging, establish and maintain a quality management system, keep detailed technical documentation and automatically generated logs, undergo the necessary conformity assessment, draw up the EU declaration of conformity, affix the CE marking, comply with registration obligations, take corrective actions in case of non-conformity, and cooperate with competent authorities. Article 26 specifies the obligations of deployers of high-risk AI-powered connected products, which include using the AI system in accordance with its intended purpose and the provider's instructions, ensuring that the input data is relevant and sufficiently representative, monitoring the operation of the AI system, maintaining the automatically generated logs (if under their control), informing any affected workers or end-users about the use of the high-risk AI system, and ensuring that personnel using the system have received adequate training.

The AI Act places distinct but interconnected obligations on both providers and deployers of high-risk AI in connected products, emphasizing shared responsibility for ensuring safety and compliance throughout the product lifecycle. Articles 16 and 26 clearly delineate the responsibilities of each actor in the value chain, reflecting the understanding that ensuring the responsible development and use of AI requires efforts from both those who create the technology and those who put it into practice. Recitals 80, 85, and 87 provide further context on the allocation of responsibilities along the AI value chain, particularly in cases where the high-risk AI system is integrated as a safety component into a product subject to other EU harmonization legislation.

5.3. Prohibited AI Practices

Article 5 of the AI Act lists a set of AI practices that are considered to pose an unacceptable risk and are therefore prohibited within the EU. These practices include the deployment of AI systems that use subliminal techniques to materially distort a person's behavior, exploit vulnerabilities of individuals due to age, disability, or socio-economic situation, perform social scoring, make risk assessments of natural persons to predict criminal behavior based solely on profiling, create or expand facial recognition databases through the untargeted scraping of the internet or CCTV footage, infer emotions of a person in the workplace or educational institutions (with limited exceptions), and use real-time remote biometric identification in publicly accessible spaces for law enforcement purposes (again, with specific exceptions).

Companies developing AI for connected products must conduct thorough due diligence to ensure their products do not engage in any of the prohibited practices outlined in Article 5, as these carry the most severe penalties for non-compliance. Prohibited practices highlight the strict nature of these prohibitions and the potential for significant fines for violations. For example, AI-powered toys that exploit the vulnerabilities of children to encourage purchases or connected devices used for social scoring based on user behavior would be strictly prohibited under the AI Act.

06. The Broader Regulatory Framework: Intersecting EU Legislation

6.1. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) remains a critical piece of legislation for AI-powered connected products that process personal data. The GDPR establishes a framework for the lawful and fair processing of personal data, based on principles such as lawfulness, fairness, transparency, data minimization, purpose limitation, accuracy, storage limitation, integrity, and confidentiality. Key requirements under the GDPR include the need to identify a legal basis for processing personal data, such as the data subject's consent or the legitimate interests of the data controller. Data subjects are also granted various rights, including the right to access their personal data, to rectify inaccuracies, to have their data erased under certain circumstances, and to object to processing.

Furthermore, organizations processing personal data must implement appropriate technical and organizational measures to ensure data security and must have procedures in place for reporting data breaches to the relevant supervisory authorities.

Compliance with the GDPR is a fundamental prerequisite for AI-powered connected products that handle personal data, and companies must ensure their data processing activities align with GDPR principles and requirements. The AI Act explicitly clarifies that the GDPR always applies when personal data is processed in the context of AI systems, reinforcing the need for companies to consider both regulations in their compliance efforts. The concurrent applicability of GDPR highlights that the AI Act's requirements are in addition to, and do not replace, the obligations under the GDPR.

Moreover, for certain high-risk AI systems, the AI Act requires providers to conduct a Fundamental Rights Impact Assessment (FRIA), which builds upon the Data Protection Impact Assessment (DPIA) mandated by the GDPR, further highlighting the interconnectedness of these regulations.

6.2. Cybersecurity Act

The Cybersecurity Act (Regulation (EU) 2019/881) aims to enhance the cybersecurity of network and information systems across the European Union. This legislation establishes the European Union Agency for Cybersecurity (ENISA) and provides a framework for the creation of European cybersecurity certificates for products and services. The Cybersecurity Act is highly relevant to the security of connected products, particularly those incorporating AI, as it emphasizes the need for robust cybersecurity measures to protect against vulnerabilities and cyber threats.

Ensuring the cybersecurity of AI-powered connected products is paramount, not only for compliance with the Cybersecurity Act but also for protecting users, their data, and the integrity of the AI systems themselves. The focus of these regulations is on the security of connected devices, emphasizing the need for security by design and default. The Cybersecurity Act and the AI Act are complementary, with the former focusing on the security aspects that are crucial for the safe and ethical operation of AI systems in connected products.

Furthermore, the Cyber Resilience Act (CRA), which entered into force on December 10, 2024, and will become applicable in 2026, further strengthens the cybersecurity requirements for connected devices, including those with AI, by mandating security by design and default throughout the product lifecycle.

Notably, the CRA explicitly states that digital products with embedded AI that qualify as high-risk AI systems under the AI Act will be considered compliant with the AI Act's cybersecurity requirements if they meet the corresponding requirements of the CRA. This demonstrates a move towards regulatory coherence, ensuring that companies addressing the cybersecurity requirements of the CRA will also meet the relevant security obligations under the AI Act.

6.3. Consumer Protection Laws

A range of consumer protection laws are also relevant to AI-powered connected products, including the General Product Safety Regulation (GPSR) (Regulation (EU) 2023/988) and the Product Liability Directive (Directive 85/374/EEC, which was replaced by a revised Directive (EU) 2024/2853 in December 2024, applicable from December 2026). These laws apply to AI-powered connected products, particularly concerning product safety, liability for defective products (including software and AI systems), and the rights of consumers regarding information and redress.

The revised Product Liability Directive explicitly applies to software, including standalone software and AI systems, making manufacturers liable for damages caused by defective AI in connected products. Existing consumer protection laws, particularly the evolving Product Liability Directive, are increasingly holding manufacturers accountable for the safety and performance of AI within connected products, emphasizing the importance of robust testing and quality assurance. The revised Product Liability Directive's application to AI includes the introduction of a presumption of causality in certain cases, which can simplify the process for victims seeking compensation for AI-induced harm.

The GPSR, applicable from December 13, 2024, focuses on ensuring the safety of consumer products placed on the EU market, regardless of the manufacturer's location. It includes specific provisions relevant to connected products, such as the requirement to provide security updates to minimize cybersecurity risks and to ensure that products are developed in a way that poses no risks to consumers, even through software errors or security vulnerabilities.

The GPSR also introduces the "*responsible person*" requirement, mandating that a designated entity within the EU (which could be the manufacturer, importer, authorized representative, or fulfillment service provider) is accountable for product compliance and safety, including for connected products with AI. The GPSR's focus on the safety of connected products, including cybersecurity aspects and the provision of necessary safety information to consumers, adds another layer of compliance for manufacturers in this sector.

07. Navigating Legal Challenges and Ensuring Compliance

7.1. Potential Legal Challenges

The integration of AI into connected products presents several legal challenges. One significant area is liability arising from autonomous decision-making by AI. Determining fault and proving causation in cases where an AI-powered connected product causes harm can be complex, particularly when the AI system is capable of evolving its decision-making over time. The autonomous nature of AI in connected products presents novel challenges for traditional legal concepts like liability and intellectual property, requiring careful consideration of responsibility and ownership in this evolving technological landscape. Complexities of liability in the context of AI, include the challenges in attributing responsibility when AI systems operate with limited human oversight.

Intellectual property rights also pose challenges, particularly concerning the training data used to develop AI models and the ownership of outputs generated by AI systems. Questions arise regarding copyright infringement in the context of training data and the patentability of AI-assisted inventions.

Ethical considerations are another critical aspect, including the potential for algorithmic bias to lead to discriminatory outcomes and the need for fairness and transparency in AI decision-making processes. Ensuring ethical AI in connected products requires proactive measures to mitigate bias and promote fairness, aligning with both legal requirements and broader societal values. The ethical considerations embedded within EU law, emphasise the principles of non-discrimination and consumer autonomy.

7.2. Compliance Obligations for Companies

Companies developing, manufacturing, and distributing AI-powered connected products within the EU market face a multitude of compliance obligations stemming from the AI Act, Data Act, GDPR, Cybersecurity Act, and consumer protection laws. Navigating the complex web of EU regulations requires a holistic and integrated approach to compliance, where companies consider the interconnectedness of the AI Act, Data Act, GDPR, Cybersecurity Act, and consumer protection laws.

The various regulations address different but overlapping aspects of AI in connected products, necessitating a unified compliance strategy. Key obligations include:

- **Conduct a thorough AI inventory:** Identify all AI systems used within connected products, whether developed in-house or sourced from third parties.
- **Perform comprehensive risk assessments:** Evaluate the risk level of each AI system according to the criteria outlined in the AI Act, paying close attention to potential impacts on health, safety, and fundamental rights.
- **Establish robust data governance and cybersecurity frameworks:** Implement policies and procedures to ensure the quality, integrity, security, and privacy of data used by and generated from connected products with AI.
- **Implement transparency measures:** Provide clear and accessible information to deployers and end-users about the AI system's capabilities, limitations, and data processing practices.
- **Develop processes for conformity assessment:** For high-risk AI systems, establish procedures to undergo the necessary conformity assessment before placing the product on the EU market.
- **Build a strong quality management system:** Implement a system that covers the design, development, testing, and deployment of AI-powered connected products.
- **Establish post-market monitoring procedures:** Continuously monitor the performance and safety of AI-powered connected products after they are placed on the market and have processes in place for reporting serious incidents.
- **Stay informed about regulatory developments:** Actively monitor the latest guidance, interpretations, and enforcement priorities issued by EU institutions and agencies, particularly the European Commission and the AI Office.

7.3. Key Compliance Requirements Table

The following table summarizes key compliance requirements for AI in connected products under EU law.

Regulation	Key Requirement	Relevant Articles/Recitals (where applicable)	Implications for Companies
AI Act	Risk Assessment	Article 9, Annex III	Identify and mitigate risks associated with AI in connected products.
	Transparency Obligations	Articles 13, 50; Recitals 6, 72, 171	Provide clear information to deployers and end-users about AI capabilities, limitations, and data processing. Inform users they are interacting with an AI system.
	Conformity Assessment	Article 43; Recital 78	Undergo mandatory assessment for high-risk AI systems before market entry, often involving third-party bodies.
	Obligations of Providers	Article 16; Recitals 80, 85, 87	Ensure compliance, provide contact info, establish quality management, maintain documentation and logs, obtain CE marking, register the system.

	Obligations of Deployers	Article 26; Recitals 80, 85, 87	Use system as intended, ensure relevant input data, monitor operation, maintain logs, inform affected individuals.
	Prohibition of Unacceptable AI Practices	Article 5	Ensure products do not engage in prohibited activities like social scoring or harmful manipulation.
Data Act	Data Access and Portability for Users	Article 4, Chapter II	Enable users to access and share data generated by the connected product with third parties.
	Information on Data Generation	Article 3, Chapter II	Provide users with clear information about the type, format, and volume of data their connected product generates.
GDPR	Lawful Basis for Processing Personal Data	Article 6	Identify a valid legal basis (e.g., consent, legitimate interests) for processing any personal data.
	Data Subject Rights	Articles 12-23	Respect and facilitate the exercise of data subject rights (access, rectification, erasure, etc.).
	Data Security and Breach Notification	Articles 32-34	Implement appropriate security measures and have procedures for reporting data breaches.

	Data Protection Impact Assessment (DPIA) / Fundamental Rights Impact Assessment (FRIA)	Article 35 (GDPR), Article 27 (AI Act)	Conduct assessments to identify and mitigate risks to data protection and fundamental rights.
Cybersecurity Act	Cybersecurity Requirements for Networked Products	Regulation (EU) 2019/881	Enhance the security of connected products and their underlying networks.
Cyber Resilience Act	Security by Design and Default	Regulation (EU) 2024/2847 (Applicable 2026)	Design and manufacture connected products with security as a core priority throughout the product lifecycle.
	Vulnerability Management and Security Updates	Regulation (EU) 2024/2847 (Applicable 2026)	Provide regular security updates and have processes for identifying and addressing vulnerabilities.
GPSR	General Product Safety Requirements	Regulation (EU) 2023/988 (Applicable Dec 2024)	Ensure products meet general safety requirements, including for connected products with digital elements.
	Responsible Economic Operator	Article 4, Regulation (EU) 2023/988	Designate a responsible person within the EU to ensure product compliance and safety.

Product Liability Directive	Liability for Defective Products	Directive (EU) 2024/2853	Manufacturers are liable for damages caused by defective products, including AI in connected products. The revised directive simplifies the burden of proof for victims in certain cases.

08. Guidance from EU Institutions and Agencies

Official guidance from EU institutions and agencies plays a crucial role in clarifying the interpretation and implementation of the regulatory framework governing AI in connected products.

The European Commission, particularly its Directorate-General for Communications Networks, Content and Technology (DG CONNECT), has been instrumental in drafting and explaining the AI Act and related legislation.

The European AI Office, established within the Commission, serves as a central hub for AI expertise across the EU and is tasked with supporting the implementation of the AI Act, especially for general-purpose AI models. This includes developing codes of practice, guidelines, and benchmarks for evaluating AI models and ensuring coherent application of the AI Act across Member States.

Official guidance from EU institutions and agencies, particularly the European Commission and the AI Office, will be crucial for understanding the practical implementation and enforcement of the AI Act and related regulations in the context of connected products.

The role of these bodies in providing interpretations and guidance on the AI Act's provisions, including the definition of AI systems, the classification of risk, and the obligations of providers and deployers. replace, the obligations under the GDPR.

Companies should actively monitor the publications and pronouncements of these EU bodies to stay informed about the latest interpretations and best practices for compliance. The evolving nature of the regulatory landscape necessitates continuous monitoring of official sources to ensure adherence to the most up-to-date understanding of the legal requirements.

Other relevant EU agencies, such as the European Data Protection Board (EDPB), also provide guidance on the intersection of GDPR and AI, which is particularly relevant for AI-powered connected products that process personal data. Specific guidance or interpretations related to the application of these regulations to connected products are likely to emerge as the AI Act's implementation progresses, and stakeholders should remain vigilant for such pronouncements.

09. The Current Landscape: AI in Connected Products in the European Union

AI is currently being widely adopted in various sectors of connected products within the European Union.

In the realm of smart home devices, AI powers virtual assistants that provide personalized automation and voice control, smart thermostats that optimize energy usage based on learned routines, advanced security systems with AI-driven threat detection and facial recognition, and intelligent appliances that can learn user preferences and adjust their operation accordingly.

Within industrial IoT, AI is integrated into predictive maintenance sensors that monitor equipment performance to anticipate failures, quality control systems that use AI vision to detect defects in manufacturing processes, and autonomous robots that can perform complex tasks in industrial environments.

The healthcare sector is witnessing the increasing use of AI in connected medical devices for remote patient monitoring, diagnostic tools that can analyze medical images with high accuracy, and implantable devices that use AI to optimize their function.

In the automotive industry, connected vehicles are incorporating AI for advanced driver assistance systems, intelligent navigation, and personalized infotainment experiences.

This widespread adoption indicates a significant market for AI-powered connected products within the EU, which will be subject to the new regulatory framework.

Emerging legal and regulatory trends in this landscape include increased scrutiny of high-risk AI applications across all sectors and a growing emphasis on the enforcement of transparency obligations, particularly concerning how AI systems make decisions and process data. Early enforcement actions and guidance from the EU suggest a focus on ensuring compliance with the fundamental principles of safety, fairness, and transparency in the deployment of AI in connected products.

10. Looking Ahead: Future Implications and Strategic Considerations

The evolving regulatory framework for AI in connected products in the EU has significant future implications for innovation and market access.

While the aim is to foster trust and safety, the stringent requirements of the AI Act and related legislation may also present challenges for companies involved in the development and deployment of these technologies.

The extraterritorial scope of the AI Act means that companies operating outside the EU but placing AI-powered connected products on the EU market will also need to comply with its provisions, potentially impacting global market access strategies. The EU's regulatory framework for AI in connected products, while aiming to foster trust and safety, may also present challenges for innovation and market access, requiring companies to adapt their strategies and operations to ensure compliance.

The potential impact of the AI Act on innovation, highlighting concerns about increased compliance costs and potential delays in product launches. To navigate this complex legal landscape effectively, companies should consider the strategic recommendations that we mentioned in "*7.2. Compliance Obligations for Companies*" of this whitepaper.

Proactive engagement with the evolving regulatory landscape and a commitment to building compliance into product development will be crucial for companies to succeed in the EU market for AI-powered connected products.

The phased implementation of the AI Act, with different obligations becoming applicable on various dates between February 2025 and August 2027, underscores the need for a strategic and forward-looking approach to compliance.

By prioritizing compliance from the outset, companies can not only meet their legal obligations but also build trust with consumers and gain a competitive advantage in the EU market for innovative and responsible AI-powered connected products.

11. US AI Regulation: A State-by-State Approach and Its Challenges

The US regulatory landscape concerning Artificial Intelligence within connected products is characterized by a dynamic and increasingly complex interplay between federal and state-level actions.

This environment is undergoing rapid evolution, particularly influenced by shifting administrative priorities and the accelerating pace of AI technological development. Previous Federal initiatives, such as the Biden Administration's Executive Order on "Safe, Secure, and Trustworthy Development and Use of AI," and the accompanying AI Bill of Rights, have aimed to establish overarching principles for ethical AI deployment and to mitigate potential risks. However, the absence of comprehensive, codified federal legislation has led to a fragmented regulatory space. This fragmentation is exacerbated by the fact that changes in presidential administrations, such as the transition to the Trump Administration, often lead to the revision or revocation of prior executive orders, leaving a patchwork of policy documents. Though some federal efforts remain, like Executive Orders 14141 and 14144.

In response to this federal legislative gap, US states are actively developing their own regulatory frameworks. This state-driven approach has resulted in a diverse and often inconsistent regulatory landscape, presenting significant challenges for businesses operating across state lines. State initiatives are targeting critical areas, including algorithmic bias, consumer protection, and sector-specific applications of AI in employment, healthcare and connected products.

Notable examples illustrate the diversity of state-level regulation:

- **Colorado's AI Act (Effective 2026):** This legislation mandates rigorous impact assessments and risk management protocols for high-risk AI systems.

- **Illinois:** The state has implemented targeted regulations addressing the use of AI in video employment interviews and insurance underwriting.
- **California:** California is at the forefront of AI regulation, focusing on automated decision tools and data privacy within AI contexts.
- **New York City's Local Law 144:** This local ordinance emphasizes transparency and fairness in employment, requiring bias audits and disclosures for automated decision-making.

Key trends shaping the regulatory landscape include:

- A notable increase in AI-related bills being introduced in state legislatures;
- A concentrated focus on regulating high-risk AI applications in IoT that pose potential harm to individuals or society; and
- Growing collaboration among policymakers, industry stakeholders, and experts to develop informed and effective regulatory frameworks

However, the lack of a unified federal approach continues to pose significant challenges, leading to potential regulatory inconsistencies and the ongoing struggle to keep pace with the rapid advancements in AI technology and what that looks like connected products.

12. Securing IoT: The 2020 Act, NIST Standards, and AI Integration

The Internet of Things Cybersecurity Improvement Act of 2020, a piece of federal legislation which aimed to bolster IoT device security within federal systems by directing NIST to create security standards and guidelines, and requiring OMB to align agency policies accordingly.

It mandated vulnerability management guidelines, restricted procurement of non-compliant devices, and established congressional oversight through reports from the Comptroller General. This legislation sought to create a structured framework for securing IoT devices against evolving cyber threats in federal operations.

In response to the 2020 IoT Cybersecurity Improvement Act, NIST Special Publication (SP) 800-213 was published in November 2021. This document equips federal agencies with essential guidance for implementing cybersecurity measures on IoT devices, addressing their unique risks to government information systems. While NIST SP 800-213 primarily focuses on general IoT security within federal systems, it necessitates consideration of embedded Artificial Intelligence/Machine Learning (hereinafter: AI/ML) components due to the inherent risks they introduce, especially concerning connected products.

Many modern IoT devices incorporate AI/ML capabilities for various functions, such as data analysis, predictive maintenance, and automation. This highlights new challenges for connected products as devices are now vulnerable to attacks that manipulate their AI/ML models, leading to compromised functionality or potentially malicious behavior.

Therefore it is important to note that when NIST SP 800-213 discusses IoT device security, manufacturers may need to look at including the security of any embedded AI/ML components.

Given that NIST SP 800-213 emphasizes risk assessment, it is reasonable to assume moving forward that this framework may require a comprehensive risk assessment, which would also include evaluating the security risks posed by embedded AI/ML components including data handling, security, and model manipulation.

The NIST Interagency Report (NISTIR) 8259 series offers comprehensive cybersecurity guidance for IoT device manufacturers and third-party supporters throughout the device lifecycle. It comprises three finalized documents:

- NISTIR 8259: Recommendations for IoT Device Manufacturers: Foundational Activities (May 29, 2020);
- NISTIR 8259A: Core Device Cybersecurity Capability Baseline (May 29, 2020); and
- NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline (August 25, 2021).

These documents aim to empower manufacturers with best practices and knowledge to implement robust cybersecurity measures, addressing customer security needs. By providing a core set of security features and guidance for customer-specific enhancements, the series seeks to simplify security management for users and mitigate widespread IoT device exploitation, while balancing factors like personal data protection.

Although implementation of the NISTIR 8259 series recommendations is voluntary, it serves as a widely recognized and comprehensive cybersecurity framework. NIST is actively engaged in revisiting and revising NISTIR 8259 to ensure it remains current and effective in addressing the evolving landscape of IoT cybersecurity. NIST's guidance extends to securing emerging technologies like AI and immersive tech in connected manufactured products, by providing frameworks to test AI model security. Through this, it aims to address the practical challenges of long-term IoT security, emphasizing the crucial link between cybersecurity and ongoing device support, especially given the varying lifespans of IoT components."

13. Securing Connected Devices and AI: California's Legislative Initiatives

California's SB-327, the IoT Security Law, strengthens security for internet-connected devices sold in the state.

It mandates "reasonable security features," requiring either unique preprogrammed passwords or user-generated authentication, particularly for devices connecting beyond local networks. This law applies broadly to internet-capable devices, aiming to mitigate cybersecurity risks stemming from the proliferation of poorly secured IoT devices.

While SB-327 doesn't explicitly address AI, its security requirements could extend to AI algorithms and data processing within these connected devices. Notably, compliance is required from all manufacturers selling IoT devices in California, including original equipment manufacturers and any contracted entities involved in design and production.

Building on consumer protection, California enacted the AI Transparency Act (SB 942) on September 19, 2024. This legislation requires developers of widely used generative AI systems to embed provenance markers in their outputs. These markers, detectable through freely available tools, will allow users to identify AI-generated content, which in turn will enhance transparency in the digital content ecosystem.

14. State-Level AI Legislation in Connected Products (as of March 24, 2025)

The following table summarizes some of the state-level legislation identified that directly or indirectly addresses AI in connected products, their scope and respective EIF dates.

State	Legislation	Key Provisions	Scope	Effective Date(s)
California	IoT Security Law (SB-327)	Requires reasonable security features and unique passwords for internet connected devices.	Manufacturers of IoT devices that sell in California.	January 1, 2020

California	CCPA/CPRA	Grants consumers rights related to personal information, including opt-out rights regarding automated decision-making and profiling. Requires privacy risk assessments for high-risk processing.	Businesses that collect personal information of California residents.	January 1, 2020 (CCPA); January 1, 2023 (CPRA)
California	AI Transparency Act (SB942)	Requires generative AI systems with over 1M monthly visitors to provide AI detection tools and disclose AI-generated content with manifest and latent disclosures.	Providers of publicly accessible generative AI systems with over 1M monthly visitors in California.	January 1, 2026
Colorado	Anti-Discrimination in AI Law (ADAI) (SB 24-205)	Protects consumers from algorithmic discrimination in consequential decisions made by high-risk AI systems. Requires disclosures to consumers interacting with AI.	Developers and deployers of high-risk AI systems making consequential decisions for Colorado consumers. Also applies to any AI system intended to interact with consumers in Colorado.	February 1, 2026

Colorado	Colorado AI Act (CAIA) (SB 24-205)	Imposes obligations on developers and deployers of high-risk AI systems, including reasonable care to avoid algorithmic discrimination, documentation, disclosures, risk analysis, and impact assessments.	Developers and deployers of high-risk AI systems operating in Colorado.	February 1, 2026
Oregon	IoT Security Law (HB 2395)	Similar to California SB-327, requires unique passwords and other reasonable security measures.	Manufacturers of consumer connected devices sold in Oregon.	2020
Virginia	High-Risk AI Developer and Deployer Act (HB 2094)	Aims to prevent algorithmic discrimination by imposing requirements on developers and deployers of high-risk AI systems making consequential decisions. Requires a duty of care, disclosure, and risk management.	Developers and deployers of high-risk AI systems making consequential decisions about Virginia residents.	July 1, 2026 (if signed by Governor). This is currently a very active ongoing bill which Compliance & Risks are monitoring daily.

15. Looking Ahead: Future Implications and Strategic Considerations

Existing regulatory frameworks predominantly address AI security within the Internet of Things (IoT) domain.

However, in certain US states, broader Artificial Intelligence legislation is beginning to impact the deployment of AI in connected products, particularly concerning data protection, security features and algorithmic decision-making.

While comprehensive legislation explicitly targeting the intersection of AI and connected products remains limited at both a federal and state level, current laws and emerging trends provide valuable insights into the evolving regulatory landscape, as evidenced by the state legislation summarized in the preceding table. State AI legislation addresses core issues such as data privacy, accountability, transparency, and algorithmic bias, especially in government applications. Despite the active regulation of AI by various states, the specific application to connected products is still in its developmental phase, with several key trends emerging in the US.

These trends include a strong national policy focus on AI innovation and global competitiveness, a tendency towards reactive rather than proactive regulation to encourage growth, and an active competition with nations like China in AI development. Despite the push for innovation, ethical considerations regarding AI bias and privacy persist.

These trends highlight several key challenges in AI regulation for connected products within the US. The absence of a unified federal AI law leads to regulatory fragmentation, resulting in inconsistent state and sectoral regulations that increase compliance burdens. Addressing the ethical implications of AI, particularly bias and privacy, remains a complex undertaking. Maintaining US competitiveness requires continued investment in AI development and the integration of AI into connected products raises concerns about the impact on the

workforce, including potential shifts in skill valuation, increased wage pressure, and even the possibility of things like enhanced worker surveillance through these interconnected systems.

It is well accepted that robust computing and data storage infrastructure are crucial for AI deployment and the rapid pace of technological evolution poses a significant challenge for regulatory adaptation. Businesses face substantial compliance costs in developing compliance programs, managing data governance, and conducting audits - particularly with the move towards risk based frameworks and their subsequent auditing and ongoing cost. Following on from that, it's important the manufacturers keep pace with evolving AI standards and best practices which requires continuous adaptation and industry collaboration.

Overall, it's anticipated that state-level regulation of AI within connected products will increase in granularity and prevalence, with precedent-setting states influencing subsequent legislative efforts such as California and Colorado - requiring companies to closely monitor these state-level developments and prepare for a potentially fragmented, yet increasingly stringent, regulatory future.

Want to gain further insights into how different jurisdictions are addressing AI-related challenges?

Watch our webinar-on-demand '**Bird's Eye View of Global AI Regulations: US, EU, UK, Singapore and China**'.

Compliance & Risks

OUR NUMBERS

300+

CUSTOMERS WORLDWIDE

195

COUNTRIES COVERED

100,000+

REGULATIONS

→ | complianceandrisks.com