

KEY REGULATIONS AND POLICIES SHAPING DIGITAL TRANSFORMATION OF THE ENERGY INDUSTRY

9th ANNUAL
BUSINESS SUMMIT

**GO DIGITAL
ENERGY**

3-4 June 2025

Amsterdam, Netherlands

WHAT IS THIS REPORT ABOUT

In this comprehensive report the Go Digital Energy analytical team outlines key EU regulations and policies that are shaping the digital transformation of the energy industry.

It highlights critical areas such as data protection, cybersecurity, and the integration of AI, emphasizing the importance of compliance and strategic planning.

The information provided is essential for energy businesses navigating the complexities of digitalization in the European Union.



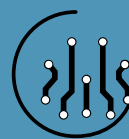
**Data:
Protection,
Standardization,
Transmission,
Storage**



Cybersecurity



**Artificial
Intelligence**



**Market Transparency
and Consumer
Protection**



INTRODUCTION

The number of active IoT devices in the world is expected to grow rapidly and surpass 25.4 billion by 2030 ([source](#)). For the EU, this process is of particular importance due to the large-scale green transition of the energy sector. To achieve its objectives, Europe needs to build an entirely new infrastructure that is much smarter and more interactive than it is today. To fit seamlessly into this infrastructure, energy businesses need to adopt more decentralized, digitalized, flexible, and clean technological approaches.

Moreover, modernization-induced challenges for the energy system—such as increased complexity and volatility, reduced predictability, safety concerns, and control issues—must be addressed.

This makes it almost impossible for companies to stay away from the digitalization process in the EU and encourages them to take action. Almost 39% of global O&G companies pursue digital transformation simply to remain competitive with their peers.

Businesses see digitalization as an opportunity to boost efficiency, enable faster decision-making, reduce leakages and costs, increase profits, and minimize risks. Over 70% of companies plan to invest “more” or “significantly more” in digital technologies within the next 3–5 years ([“DIGITALISATION. Challenges and opportunities”](#) by Amit Chander Gupta, 2024). It seems that postponing change is no longer an option. But where to start?

The legislative framework for energy companies in the EU is steadily becoming more complex. Any new improvement, product development, or technology implementation requires active and careful compliance with legal requirements. First, energy companies looking to digitize their business should consider the “classic” internal EU market product requirements (CE mark).

Second, they must comply with the strict legislative framework governing sustainability in the energy sector. Third, they must navigate an entirely new regulatory landscape covering AI-based technologies, data interoperability and protection, cybersecurity, and more.

In total, there are more than 100 pieces of legislation in the EU digital sector that are already in force, with a significant number in the proposal or planning stages. While not all of these policies are directly relevant to the energy sector, some are crucial, some offer useful instruments such as sandboxes and training programs, and others help identify and mitigate risks. In this report, we will briefly examine the 10 EU regulations that every energy business on the path to digitalization must consider.

STRATEGY

1. Digitalising the Energy System - EU Action Plan (DoEAP)

[The EU Action Plan on Digitalising the Energy System](#), adopted in October 2022, is a cornerstone of the European Union's strategy to integrate digital technologies into the energy sector. It provides an insight into the priorities for energy sector modernization and the main technologies that will be involved in the near future.

By 2030, the plan seeks to reduce energy consumption, improve grid flexibility, and support the integration of renewable energy sources, ensuring a sustainable and secure energy future for Europe.

Key priorities:

- promote connectivity, interoperability, and seamless exchange of data between different actors while respecting privacy and data protection;
- enhance cybersecurity;
- address energy consumption of digital technologies and promote greater efficiency and circularity;
- encourage consumers to increase control over their energy use and bills by using new digital tools and services;
- foster investments in the electricity grids;
- design an effective governance, through structural and joint planning by public authorities in cooperation with the private sector, learning of all actors involved, as well as continuous support for R&I.

Projects & technologies to be implemented:

Smart grids

Implementation of demand response programs that allow consumers to adjust their energy consumption in response to price signals. Use of IoT devices for real-time monitoring of grid conditions. Deployment of smart meters for electricity, gas, and heat.

Digital Twin

Creation of digital twins of energy-producing and consuming assets, such as buildings, power plants, pipelines, and distribution networks. Use of digital twins for simulating operations, predicting equipment failures, and optimizing maintenance schedules.

Renewable energy integration

Use of IoT/ML to forecast renewable energy generation and optimize grid operations. Development of smart charging solutions for electric vehicles that can help to balance the grid.

Development of pan-Europe energy data infrastructure

Establishment of common energy data space based on cloud and edge computing. Development of data models and standards to ensure interoperability. Implementation of secure data-sharing platforms that protect privacy and confidentiality.

Cybersecurity projects.

Implementation of robust cybersecurity measures to protect energy systems from cyberattacks. "Security-by-design" approach. Protection of cross-border energy flows. Development of incident response plans and cybersecurity awareness training programs.

Peer-to-peer energy trading

Employing blockchain for smart contracts that manage energy production in local energy communities. Using blockchain for tracking the origin of gases and electricity.

Real-life solutions & helpful links:

[InterConnect](#), the first blueprint for the Common European Reference Framework (CERF) for energy applications for consumers.

[TwinEU](#).




**DIGITAL
INNOVATIONS.
CONNECTED MINDS.
A GREENER
TOMORROW**

9th ANNUAL
BUSINESS SUMMIT

GO DIGITAL ENERGY

3-4 June 2025

Amsterdam, Netherlands

 <https://globuc.com/digitalsolutions/>

DATA: PROTECTION, STANDARDIZATION, TRANSMISSION, STORAGE

Enforced in May 2018, [the General Data Protection Regulation](#) is a comprehensive EU regulation designed to **protect personal data and privacy**. It applies to all organizations that collect, process, or store data of EU residents, regardless of where the organization is based. Key principles include transparency, data minimization, accuracy, and security while granting individuals rights such as access, rectification, and the ["right to be forgotten"](#).

2. General Data Protection Regulation (GDPR)

Enforced in May 2018, the General Data Protection Regulation is a comprehensive EU regulation designed to protect personal data and privacy. It applies to all organizations that collect, process, or store data of EU residents, regardless of where the organization is based. Key principles include transparency, data minimization, accuracy, and security while granting individuals rights such as access, rectification, and the "right to be forgotten".

Influence on the energy sector:

The energy sector particularly with the rise of smart grids and energy trading platforms generates vast amounts of personal data, such as energy consumption patterns and location data. GDPR imposes strict requirements on how this data is collected, processed, and stored, significantly impacting energy companies. The law mandates robust security measures, such as encryption and pseudonymization, to safeguard consumer data. All energy companies must inform customers about data usage, obtain consent, and allow data portability or erasure upon request.

Pros:

Increased consumer trust.

GDPR compliance fosters greater consumer trust in energy companies' data handling practices, potentially leading to stronger customer relationships and brand loyalty.

Improved data governance.

The law encourages the development of robust data governance frameworks in the energy sector, promoting consistency, better data quality, security, and accountability.

Enhanced innovation.

The regulation incentivizes the adoption of privacy-enhancing technologies, such as data anonymization and pseudonymization, which can enable data-driven innovation while protecting individual privacy.

Cons:

Increased compliance costs.

Implementing and maintaining GDPR compliance can be costly for energy companies, especially smaller ones, due to the need for specialized legal teams, data protection officers, and updated systems.

Complexity in data management

The GDPR imposes strict guidelines on how data must be collected, stored, and used, which can create operational challenges, particularly when managing large datasets common in the energy sector.

Risk of penalties.

Non-compliance with GDPR can lead to hefty fines and penalties, which could significantly impact the financial stability of an energy company..

Operational restrictions.

GDPR's strict rules on data retention and processing could limit the scope of data usage for innovative projects, potentially hindering the development of new services and technologies that rely on consumer data.

3. Data Act

The [EU Data Act](#), adopted in January 2024, aims to increase transparency and make data more usable across sectors. It facilitates the creation of Common European Energy Data Space (CEEDS) and **data sharing** among businesses, with consumers, and with governments to promote innovation and competition.

Influence on the energy sector:

The act applies to both personal and non-personal data generated by connected products, such as smart meters and industrial IoT devices, making it highly relevant to the energy sector.

Pros:

Enhancing grid efficiency.

By facilitating data sharing between transmission system operators (TSOs), distribution system operators (DSOs), and other stakeholders, the Data Act supports the development of smart grids and digital twins of the electricity network.

Accelerating digitalization through interoperability and standardization.

The Act mandates the development of interoperable standards, ensuring that common data formats and APIs can be shared seamlessly across different systems and sectors.

Driving innovation.

The Act encourages the development of new business models, such as energy-as-a-service and peer-to-peer energy trading. Startups and SMEs can leverage shared data to create innovative solutions, fostering a more competitive market.

Empowering consumers.

Users of connected products have the right to access data generated by their devices. Data must be provided in a structured, machine-readable format, free of charge, and in real-time where feasible.

Cons:

High compliance costs.

Energy companies must invest in IT infrastructure and staff training to meet the Act's requirements, which can be burdensome for SMEs.

Risk of penalties

Non-compliance with the act can lead to hefty fines and penalties, which could significantly impact the financial stability of an energy company.

Risk of data misuse.

Increased data sharing raises concerns about privacy breaches and unauthorized use of sensitive information.

Complexity in implementation.

Ensuring interoperability and protecting business secrets while sharing data can be technically and legally challenging.

Potential loss of competitive advantage.

Companies that rely on proprietary data for competitive advantage may face challenges in sharing data with third parties. Safeguards for protecting trade secrets and intellectual property may not fully address these concerns.

4. Interoperable Europe Act (IEA)

[The Interoperable Europe Act](#) is aimed at **enhancing public sector interoperability across Member States**. It seeks to create a network of interconnected digital public administrations to streamline cross-border services, reduce administrative burdens, and foster innovation. The Act entered into force in April 2024.

Influence on the energy sector:

The IEA has significant implications for the energy sector, particularly for smart grids and cross-border energy data flows. The act facilitates seamless connected devices' data exchange between energy stakeholders, enabling better grid management and integration of IoT-enabled energy facilities.

Pros:

Improved grid management.

Interoperability enables real-time data sharing, enhancing grid resilience and efficiency.

Cost Savings.

Reduced administrative burdens and optimized energy systems lead to significant cost savings for energy companies and consumers.

Innovation opportunities.

The act fosters innovation in energy technologies, creating new business opportunities and enhancing competitiveness.

Cons:

High compliance costs.

Implementing interoperable systems and meeting reporting requirements can be costly, particularly for smaller energy companies.

Technical complexity.

Achieving interoperability across diverse energy systems and technologies requires significant expertise and resources.

Risk of data misuse.

Increased data sharing raises concerns about privacy breaches and unauthorized use of sensitive energy data.

Risk of penalties.

Non-compliance with the act can lead to hefty fines and penalties, which could significantly impact the financial stability of an energy company.

5. Energy Efficiency Directive (EED)

[The Energy Efficiency Directive](#), revised in 2023, aims to reduce the European Union's energy consumption by 11.7% by 2030. It emphasizes the role of data centers and public buildings in achieving this goal.

Data centers are required to report key performance indicators (KPIs) related to energy and water usage, enhancing transparency and efficiency. The directive promotes the reuse of waste heat and the integration of renewable energy into the grid.

Influence on the energy sector:

Energy companies manage extensive operational, geospatial, engineering, financial, and employee data. Digitalization will further increase data volumes, presenting challenges in data storage and compliance with evolving legislation.

Pros:

Enhanced energy efficiency and sustainability.

Alignment with the EU's climate neutrality objectives.

Cons:

Potential costs associated with upgrading infrastructure to meet reporting standards.

Increased administrative responsibilities.

Real-life solutions & helpful links:

Smart Appliances Reference ([SAREF](#)), a common interoperability language, a standard of the European Telecommunications Standards Institute and oneM2M—the global initiative for IoT standardization.

[SAREF4ENER](#), the SAREF extension for the energy domain.

[OPEN DEI "data lakes"](#).

[EUCloudEdgeIoT](#).

[EDDIE project](#).

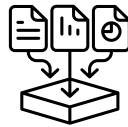
CYBERSECURITY

6. Network and Information Systems (NIS 2) Directive

The NIS 2 Directive, adopted in December 2022, is the EU updated cybersecurity legislation aimed at **strengthening the resilience of network and information systems across critical sectors, including energy**. It introduces strict cybersecurity requirements and enhances enforcement mechanisms to address growing cyber threats. The directive mandates robust risk management with penalties for non-compliance of up to 10 million or 2% of global turnover.



DEVELOPMENT OF
CYBERSECURITY RISK
MANAGEMENT POLICIES



SUPPLY CHAIN
STANDARDIZATION



INCIDENT RESPONSE PLAN
IMPLEMENTATION



AUDITS BY
AUTHORITIES



STAFF TRAINING



CRYPTOGRAPHY AND
ENCRYPTION



**JOIN GO DIGITAL ENERGY
COMMUNITY ON LINKEDIN**

Influence on the energy sector:

The energy sector is classified as an essential entity under NIS 2, making it a priority for compliance. The directive impacts the sector by:

- Enhancing cybersecurity measures. Energy companies must adopt advanced technologies to protect critical infrastructure like power grids and industrial control systems (ICS) as well as cross-border energy flows.
- Strengthening incident management. Companies are required to establish incident response plans and report significant cyber incidents to authorities within 24 hours.
- Ensuring supply chain security. Energy providers must ensure third-party suppliers meet stringent cybersecurity standards.
- Increasing regulatory oversight. National authorities will conduct regular audits, with non-compliance leading to hefty fines.
- Comprehensive staff training. The NIS 2 Directive mandates awareness as a key component of cybersecurity risk management, requiring all employees, including senior management, to undergo regular training on topics like cyber hygiene, incident handling, and supply chain security.

Pros:

Improved resilience

The legislation strengthens the sector's ability to withstand cyberattacks, ensuring continuity of essential services.

Consumer trust

NIS 2 enhances public confidence by ensuring robust data protection and incident response.

Standardization

The law harmonizes cybersecurity standards across the EU, improving cross-border collaboration.

Innovation

NIS 2 encourages investment in advanced cybersecurity technologies, fostering innovation.

Cons:

High costs

Implementing NIS 2 requirements can be costly, especially for smaller energy companies.

Risk of penalties

Non-compliance with the directive can lead to significant fines and penalties, which could significantly impact the financial stability of an energy company.

Technical complexity

Upgrading legacy systems and ensuring supply chain security can be challenging.

Administrative burden

Reporting and auditing requirements increase administrative workloads.

Regulatory uncertainty

Differences in national implementations may create compliance challenges for cross-border operations.

7. Cyber Resilience Act (CRA)

[The Cyber Resilience Act](#), entered into force in December 2024, is an EU regulation designed to **enhance the cybersecurity of digital products, both hardware and software, throughout their entire lifecycle.**

Aiming to establish a baseline of cybersecurity standards for digital products placed on the EU market, the CRA shifts the focus from voluntary standards to legally binding obligations for manufacturers, importers, and distributors.

Influence on the energy sector:

The CRA's influence on the energy sector encompasses digital products integral to energy infrastructure. This includes smart meters, industrial control systems (ICS), IoT devices used for monitoring and control, etc. By mandating cybersecurity requirements for these products, the CRA seeks to minimize vulnerabilities and bolster the overall security of the sector, making it more resilient against evolving cyber threats.

Pros:

Enhanced security posture

The CRA mandates cybersecurity measures that promote due diligence and require manufacturers to disclose security information, thereby strengthening overall security.

Increased trust.

Providing tools and training for energy sector employees enhances their understanding of cybersecurity, fostering greater trust in the adoption of new technologies, such as AI.

Cons:

Higher costs for manufacturers

Implementing regulations can be expensive to uphold.

Innovation may be hindered

The costs associated with compliance may discourage innovation, as manufacturers might focus more on meeting regulatory requirements than on developing new technologies.

Complexity and compliance burdens

Expertise is needed in order to correctly implement and uphold requirements.

Risk of penalties

Non-compliance with the act can lead to significant fines and penalties, which could significantly impact the financial stability of an energy company.

Real-life solutions & helpful links:

[Network Code on Cybersecurity for Cross-Border Electricity Flows.](#)
[European Energy Information Sharing & Analysis Centre.](#)

ARTIFICIAL INTELLIGENCE

8. Artificial Intelligence Act (AI Act)

Adopted in March 2024, the [EU Artificial Intelligence Act](#) establishes a unified legal framework for AI across the EU. It employs a risk-based approach, categorizing AI systems depending on their potential to cause harm.

High-risk AI systems must meet stringent requirements related to data quality, transparency, human oversight, and cybersecurity, fostering innovation while safeguarding health, safety, and EU fundamental rights & values.

Influence on the energy sector:

The EU AI Act has a significant impact on the energy sector, affecting applications such as grid optimization, predictive maintenance, energy trading, and fraud detection. Given that the energy sector is classified as critical infrastructure, AI systems used by energy companies are considered high-risk.

Consequently, these systems must meet stringent requirements, including ensuring data quality, transparency in algorithmic decision-making, and implementing human oversight.



Pros:

Increased trust.

Ethical and transparent AI will foster public trust, promoting greater adoption of AI-powered energy services.

Responsible innovation

A clear legal framework guides companies in prioritizing safety, fairness, and transparency in AI development.

Risk reduction

Risk assessments and mitigation measures will help address potential harms, such as bias and security vulnerabilities.

Competitive advantage

Companies adopting responsible AI practices may attract customers, investors, and talent.

Support and resources

The act provides the companies with resources and a legal framework for testing, adjusting, and improvement of AI systems.

Among other things, sandboxes provide a legal basis for reprocessing personal data in the public interest, while codes of conduct allow the application of requirements for high-risk AI systems to non-high-risk AI systems.

Cons:

Innovation delays

Strict requirements for high-risk systems may hinder the rapid deployment of new AI-powered energy solutions.

Compliance costs

Implementing and maintaining compliance can be costly and complex, especially for companies lacking internal AI governance.

Legal uncertainty

The act's interpretation and enforcement remain unclear, adding uncertainty for businesses.

Complex scope

Unique AI applications may complicate risk classification. Additional regulation is to be provided in the near future.

Skills shortage

The lack of AI engineers in the industry could slow implementation efforts.

Penalties.

The AI Act includes a robust system of penalties for non-compliance.

Real-life solutions & helpful links:

[HEDGE-IoT.](#)
[ODEON.](#)
[I-ENERGY.](#)

MARKET TRANSPARENCY AND CONSUMER PROTECTION

9. Digital Services Act & Digital Markets Act

The Digital Services Act and Digital Markets Act, entered into force in November 2022, are EU regulations designed to **ensure fair competition and transparency in digital services**.

They mandate algorithmic transparency, protect users from harmful content, and enforce antitrust rules for platforms designated as “gatekeepers.”

Influence on the energy sector:

As blockchain-based peer-to-peer energy trading evolves, these acts increasingly affect the energy sector.

Pros:

Market access.

DSA and DMA provide standardized rules for EU-wide market entry.

Enhanced trust

Legislations increase user confidence in digital platforms.

Leveled the playing field and boosted innovation

Acts promote fair competition, benefiting digital energy startups.

Cons:

Compliance costs

Implementing these regulations can be expensive.

Regulatory complexity

Navigating cross-border operations may be challenging.

Potential fines

Non-compliance can result in significant penalties, up to 10% of global turnover under the DMA.

Real-life solutions & helpful links:

[Electricity Directive](#), also containing useful information on transparency and consumer protection in the energy sector.

[Powerledger](#), the blockchain-based energy trading platform.

[Digital Tools for Energy Communities](#).



CONCLUSIONS

Digitalization is imperative

The modernization of the European energy grid and green transition demand digitalization within the sector. Postponing these changes is no longer an efficient strategy.

Compliance is complex

Navigating the EU regulatory landscape is intricate, requiring careful attention to established product requirements, sustainability regulations, and emerging digital legislation.

Data is central

Data interoperability, protection, and management are critical for success. These areas are heavily shaped by the General Data Protection Regulation (GDPR) and the Data Act, which set the standards for how data should be handled and shared.

Cybersecurity is paramount

The energy sector is a critical infrastructure, making cybersecurity a top priority. This is governed by the NIS 2 Directive and the Cyber Resilience Act. Robust security measures, well-developed incident response plans, and supply chain security are essential components.

AI requires careful governance and further clarification

The AI Act introduces specific requirements for energy systems as high-risk systems placing a strong emphasis on data quality, transparency, and human oversight to ensure the responsible use of AI. In the meantime, the concept of risk evaluation requires additional regulation.

Collaboration and learning are crucial

A whole value chain approach is essential, encouraging collaboration between public authorities, consumers, and the private sector. Continuous learning and support for research and innovation are also vital for ongoing success.

DIGITAL INNOVATIONS. CONNECTED MINDS. A GREENER TOMORROW



9th ANNUAL
BUSINESS SUMMIT

GO DIGITAL ENERGY

3-4 June 2025

Amsterdam, Netherlands



<https://globuc.com/digitalsolutions/>