

# ROLE OF DIGITALIZATION AND ITS IMPACT ON CONSUMER ISSUES

*Empowering Mediterranean regulators for a common  
energy future*

REF: MED21-32GA-4.11



Consumer  
Working Group  
(CUS WG)



Co-funded by  
the European Union

## ABSTRACT

This document presents the role of digitalization and its impact on consumer issues as part of the Consumers Working Group's (CUS WG) 2021 action plan.

The report aims to explore how digitalization will support the development of smarter energy. Digital solutions will help consumers better manage their consumption but also increase their awareness on how their behavior can impact the market.

## AKNOWLEDGMENTS

This report is the result of a project carried out by the MEDREG Consumer Working Group (CUS WG). MEDREG wishes to thank the CUS Working Group for their contribution and efforts.

*Main drafters: Igor Telebak (REGAGEN, Montenegro), Andre Buttigieg (REWS, Malta), and Erjola Sadushi (ERE, Albania).*

*Co-drafters: Bardhi Hoxha and Zitouni Lamine Abdelkader (MEDREG Secretariat)*

If you have any queries regarding this paper, please contact:

MEDREG Secretariat

Email: [info@medreg-regulators.org](mailto:info@medreg-regulators.org)

## DISCLAIMER

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of MEDREG and do not necessarily reflect the views of the European Union.

## ABOUT MEDREG

MEDREG is the association of Mediterranean energy regulators, bringing together 27 regulators from 22 countries that span the European Union (EU), the Balkans, and North Africa.

MEDREG acts as a platform for facilitating information exchange and providing assistance to its members in addition to fostering capacity development activities through webinars, training sessions, and workshops.

Mediterranean regulators work together to improve the harmonization of regional energy markets and legislations, seeking a progressive market integration in the Euro-Mediterranean Basin.

Through constant cooperation and information exchange among members, MEDREG aims at fostering consumer rights, energy efficiency, infrastructure investment, and development by employing safe, secure, cost-effective, and environmentally sustainable energy systems.

The MEDREG Secretariat is located in Milan, Italy.

For more information, visit [www.medreg-regulators.org](http://www.medreg-regulators.org)

## Executive summary

The energy sector is on the cusp of a new era, dominated by new technologies and the digitalization of all its levels (generation, transmission, distribution, and consumption). Many countries have already started to use new technologies and innovative solutions to upgrade the efficiency of their energy systems such as by implementing smart meters, including automatization in the transmission and distribution networks, and employing electrical vehicles.

In this report, we focus on the role of digitalization and its impact on consumer issues in the Mediterranean region. In that perspective the analysis will be divided into five chapters, starting with an understanding of the digital channels and the availability of information for consumers, followed by a chapter dedicated to the most common digitalization technologies such as smart technology and small-scale distributed electricity resources, and a chapter dedicated to cyber security.

The report concludes with a summary of the main findings and recommendations based on the analysis of the data collected from the members.

# TABLE OF CONTENT

Executive summary	3
<b>INTRODUCTION</b>	<b>6</b>
<b>DIGITAL CHANNELS AND INFORMATION</b>	<b>8</b>
2.1. Digital communication and services at national regulatory authorities' (NRAs) level	11
2.2. Digital communication at the distribution system operator (DSO) level	13
2.3. Digital communication at the suppliers' level	15
<b>SMART TECHNOLOGIES</b>	<b>17</b>
3.1. Smart meters	18
3.2. Distributed electricity generation	20
<b>OVERVIEW ON CYBERSECURITY IN THE MEDITERRANEAN REGION</b>	<b>22</b>
<b>CONCLUSIONS</b>	<b>26</b>
<b>ANNEXES</b>	<b>28</b>
Annex 1: National competent authorities designated to monitor/coordinate the implementation of the strategy	29
Annex 2: Cybersecurity standards	30





Nowadays, digital technology is constantly used in our daily lives, and consumers are becoming more demanding in terms of information and developing more user-friendly solutions.

For this report, a survey has been circulated among the member to obtain the required data for analyzing the role of digitalization and its impact on consumer issues.

Out of the 27 members, 17 members replied positively to the questionnaire, five didn't provide responses, and five other members reported that the questionnaire is not applicable for them (Tunisia, Libya, Jordanian Ministry, Moroccan Ministry, and Algeria's "ARH"), as represented in the following figure. This report presents data on the MEDREG members that responded to the questionnaire.

Furthermore, MEDREG's members discussed the challenges that digitalization will bring to the drafting of regulations in this new technological era in a training that addressed four main concepts: flexibility, open data platforms, data usage and cybersecurity, and the growing role of consumers in shaping energy markets.

The training demonstrated the key role of digitalization in fostering decarbonization and incorporating renewable sources in energy systems. It also presented the challenges and solutions that digitalization will bring to the regulators<sup>1</sup>.



Figure 1. Overview of the replies to the CUS WG questionnaire

<sup>1</sup> See MEDREG's report on "Digitalization Training"



A digital era is emerging in the energy market, and it represents a new opportunity to use energy systems in a more efficient, clean, and economic way. Digital technologies allow the use of new mechanisms and measures that are not possible with the traditional network. Employing smart meters, demand response management, and electric vehicles provides a further solution to achieve energy transition and, simultaneously, requires the use and analysis of a significant amount of data and information.

From the consumers' point of view, the availability of information regarding their energy consumption helps them understand their impact and role in the energy systems. This chapter will provide an overview of the available digital channels and information relevant to consumers at different levels (regulators, distributors, and suppliers).

The definition of “electronic communication” is not always provided in the law. The survey shows that 7 out of 17 members have a definition for “electronic communication” in their legislation, and even fewer in the energy sector legislation.

The following table provides the legislation that defines “electronic communication” for each member.

Table 1. Electronic communication legislation

Country	Regulator	Definition of “electronic communication” in the legislation	
		Yes	No
Albania	ERE	Law nr. 97/2013 on audiovisual media in the Republic of Albania	
Algeria	CREG	<ul style="list-style-type: none"> <li>• Law No.18-04 of 10 May 2018.</li> <li>• Executive Decree No. 21-44 of 3, corresponding to January 17, 2021,</li> <li>• Executive Decree <b>No. 18-246</b> of 29, corresponding to October 9, 2018</li> <li>• Decision No. 61 / SP / PC / ARPCE / 2020 of December 23, 2020</li> <li>• In the energy sector: Provisions of Law no. 02-01, corresponding to February 5, 2002</li> </ul>	
Cyprus	CERA	Law on the Regulation of Electronic Communications and Postal Services of 2004	
Egypt	EgyptERA		
Egypt	GASREG	Executive regulation and law and licenses	
France	CRE	There is a legal definition in Article L.32 of the Postal and Electronic Communications Code (Code des Postes et des Communications Électroniques). Electronic communications "means the emission, transmission or reception of signs, signals, writing, images or sounds by electromagnetic means."	
Greece	RAE		
Israel	PUA	A consumer can send a message by any digital means, such as via fax, e-mail, the internet, text message, etc. It will be seen that the notice was received by the consumer after 72 hours from the date of its production and dispatch.	
Italy	ARERA	Primary law – Electronic Communications Code, Legislative Decree 1 no. 259 of August 2003	
Jordan	EMRC		

Country	Regulator	Definition of “electronic communication” in the legislation	
		Yes	No
Lebanon	LCEC		
Malta	REWS		
Montenegro	REGAGEN	In energy sector legislation, there is no definition of “electronic communication,” but there is a law on electronic communication.	
Palestine	PERC		
Portugal	ERSE	The law on electronic communications (Law no. 5/2004) defines "electronic communications service" and "electronic communications network."	
Spain	CNMC	The "electronic communication" legislation is not specific for energy. The applicable legislation is: a) Law 9/2014 (General Law on Telecommunications), further developed under the detailed regulation "Electronic Communications and Public Networks Act 25/2007"; b) Law 34/2002, of July 11, 2002, on information society services and electronic commerce; c) Royal Decree 2296/2004, of December 10, 2004, approving the regulation on electronic communications markets, network access, and numbering; and d) Law 56/2007, of December 28, 2007, "Measures for the Promotion of the Information Society". Legal framework: primary.	
Turkey	EMRA	There is a definition in the law on electronic communication. Upholding this law is the responsibility of the Information Technologies and Communications Authority. In energy sector legislation, there is no definition of “electronic communication.”	

## 2.1. Digital communication and services at national regulatory authorities' (NRAs) level

The communication and availability of information at the regulators' level are crucial to raise consumer awareness regarding their rights and obligations, as well as their role in the energy systems.

The level of information shared with consumers through digital channels differs from one member country to another, e.g., from Jordan, where information related to consumers' rights and tariffs are available, to Algeria, Portugal, and Spain, where information on energy-saving and general information are additionally available. The figure below provides an overview of the available information provided to consumers at the

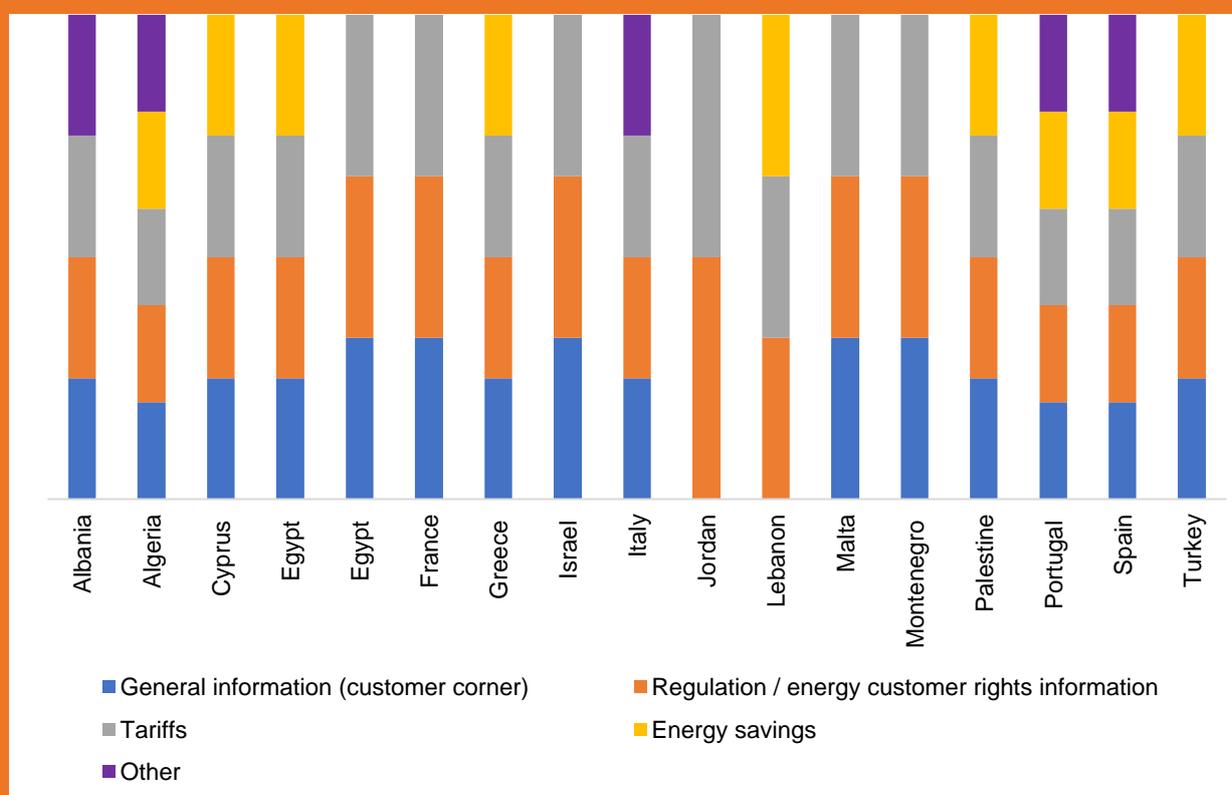


Figure 2. Information provided to consumers at the NRA level

NRA level such a dedicated consumer's corner offering general information.

Besides relevant information, digital services are available in most of the MEDREG members, from individual assistance to price comparison tools. It is also important to highlight that in some cases digital services are not available at the NRA's level but at another entity's level, for instance, in France, the CRE does not provide the price comparison tool. However, this service is available at the "Médiateur National de l'Énergie"<sup>2</sup>.

<sup>2</sup> <https://comparateur-offres.energie-info.fr/compte/profil>

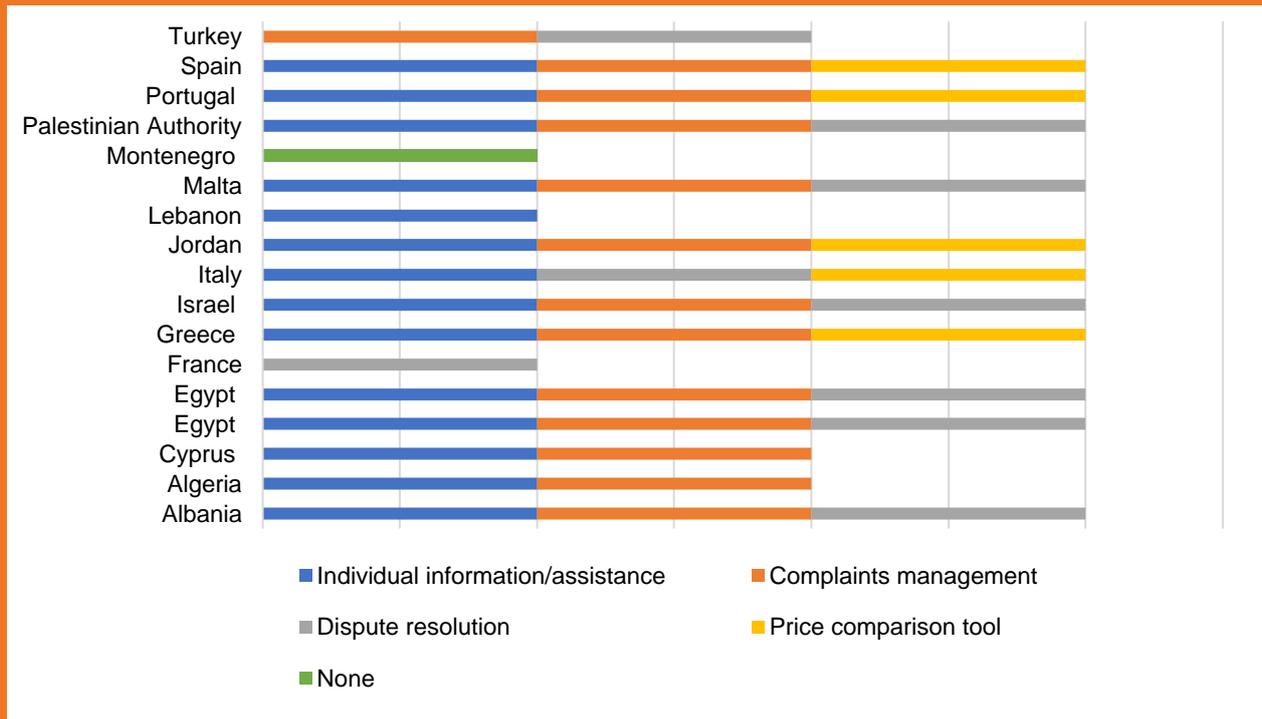


Figure 3. Digital services offered at the NRA level

Besides the availability of the information and services, the tools used to share them are important. Nowadays, social media are part of our daily lives, and they represent a direct communication channel with consumers. Thirteen members from 17 used at least one social media platform to communicate with the consumers.

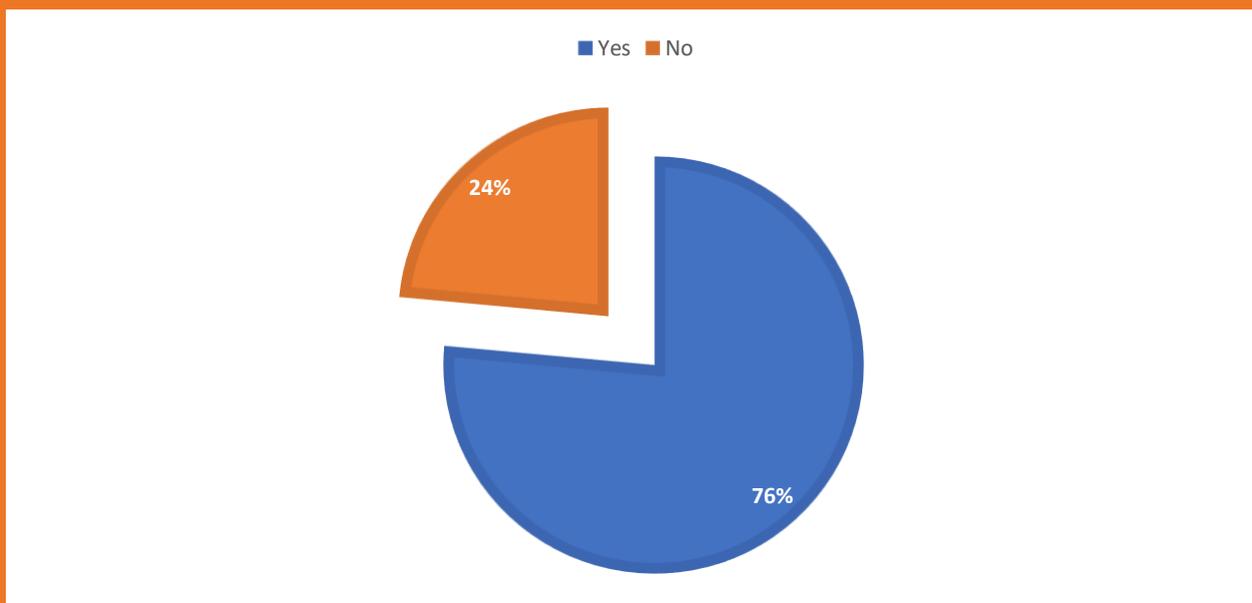


Figure 4. Use of social media by the NRA

The survey has shown that most NRAs consider that the availability of information to consumers and the use of friendly tools are important aspects that may lead to well-oriented/informed consumers that can contribute to the energy transition more efficiently.

## 2.2. Digital communication at the distribution system operator (DSO) level

At the DSO level, the availability of information and transparency are critical issues. The information provided must be well-chosen and consumer-friendly so that the consumer has the necessary information regarding their consumption and the quality of service, without being bombarded with complex and excessive data. Across the Mediterranean region, DSOs use at least one consumer communication channel (webpages, social media, direct mailing, newsletters, etc.). In most cases, all communication channels are available; furthermore, some DSOs use additional tools such as call centers and SMS and mobile applications.

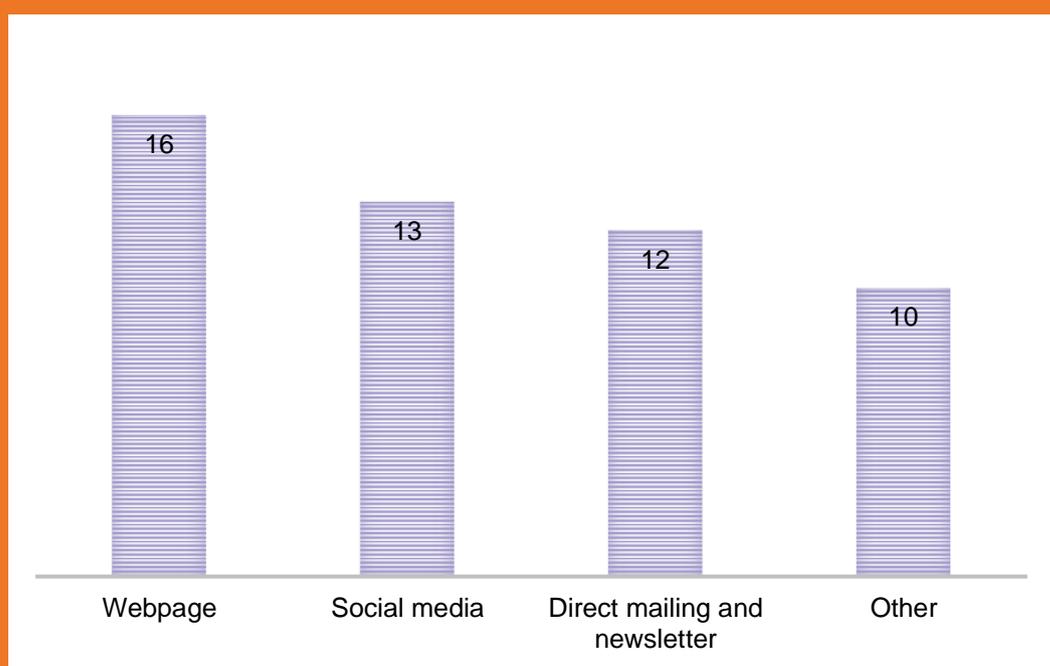


Figure 5. Use of social media by the DSOs

In addition to the open digital channels established with consumers, DSOs facilitate access to services and information by making them available online. Their main services are related to the grid connection information process, relevant data such as consumption, communication in case of disturbance or outages, and the availability of online support.

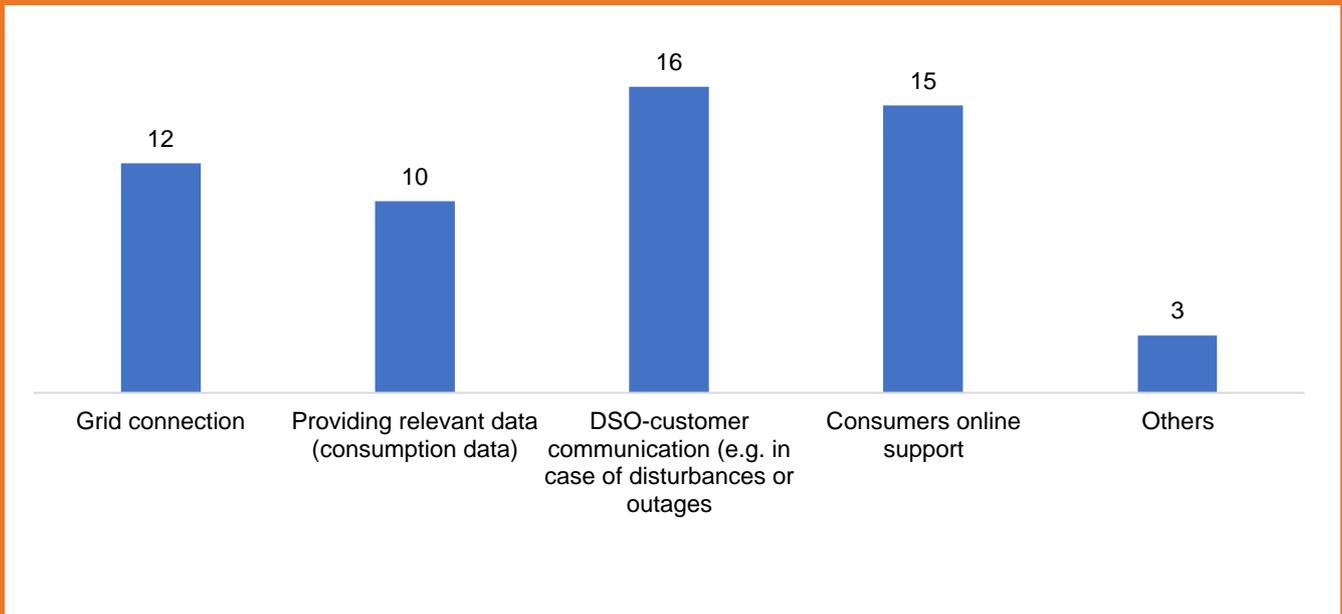


Figure 6. Main online services provided by DSOs

With regard to grid connection, even though the information concerning the process and the steps to follow are usually available online, in only 7 countries (mostly in the EU countries, Algeria, and Israel) can the application for a new connection be done online.

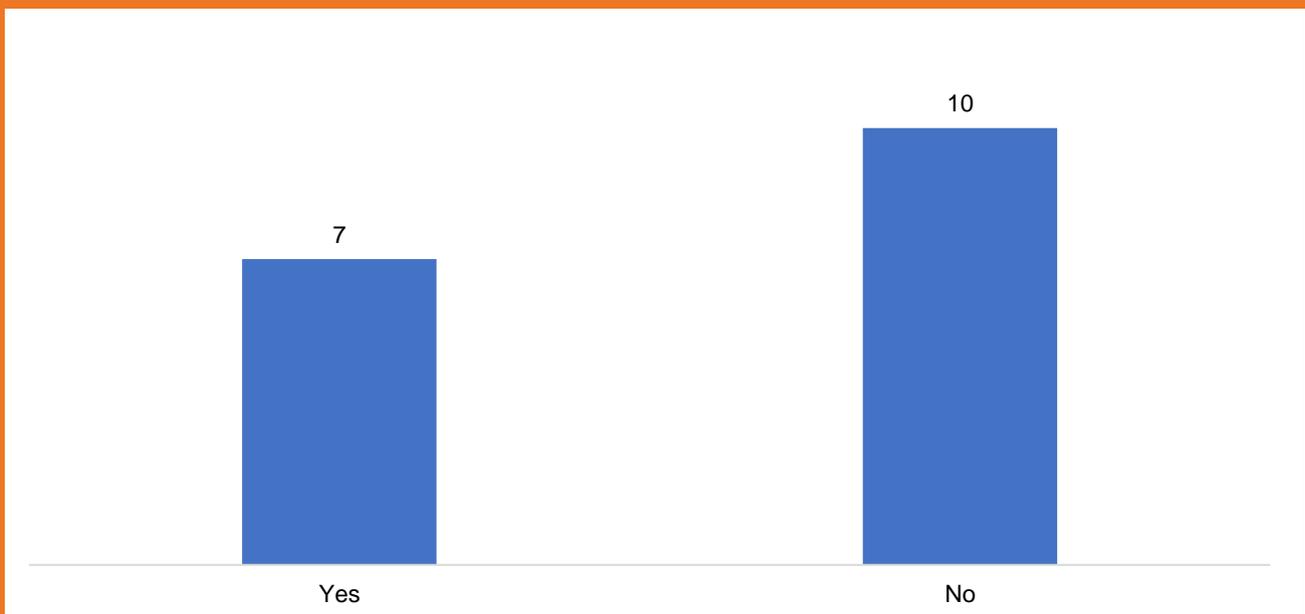


Figure 7. Online application for new connection

At the DSOs' level, all digital channels and tools may be used to comply with the obligations of the DSOs toward consumers' rights for information and services. The second reason could pertain to the consumer expectations for customer services and user-friendly tools. In addition, it may help improve the efficiency of operations, reduce costs, and facilitate the contact with end-consumers.

### 2.3. Digital communication at the suppliers' level

In most countries, consumers have the option to choose their suppliers; therefore, the competitiveness between suppliers is very high. Hence, to attract more customers, digital communication tools and user-friendly mobile applications are used.

The survey shows that several online services are available for consumers at the supplier's level and that most clients (in 14 out of the 17 countries) can make requests to suppliers electronically through the supplier's website, by using a mobile device application, or by email.

The following figure provides an overview of the main online services available for consumers at the supplier's level.

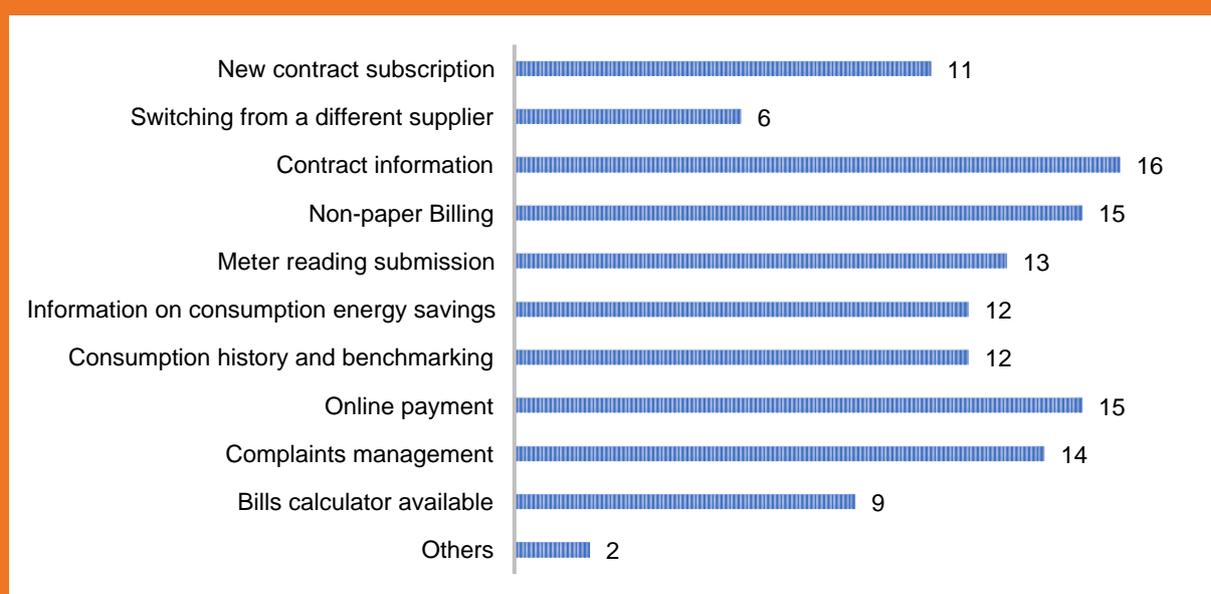


Figure 8. Online services suppliers usually offer customers

Today, the presence of mobile devices in our everyday lives and activities is undeniably beneficial. The availability of mobile apps is on an increase such that it produces a noticeable change in the way humans feel and experience computing.

In energy systems, suppliers have developed many apps to provide services and real-life information to their consumers, and the most basic services in suppliers' mobile applications are bill display and bill payments; in some suppliers' mobile applications, more advanced services such as providing energy usage information are available.

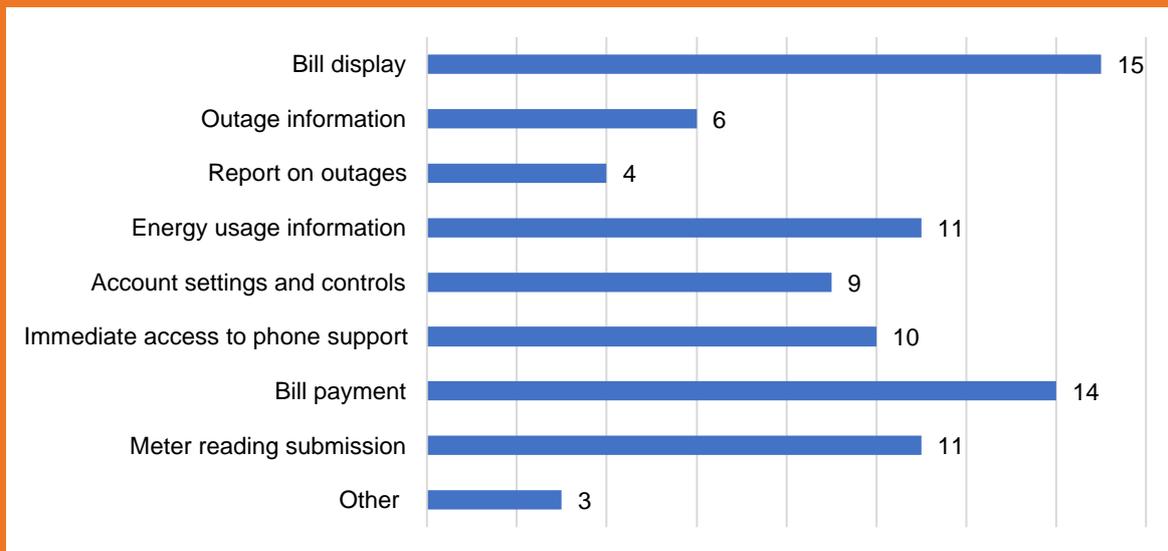
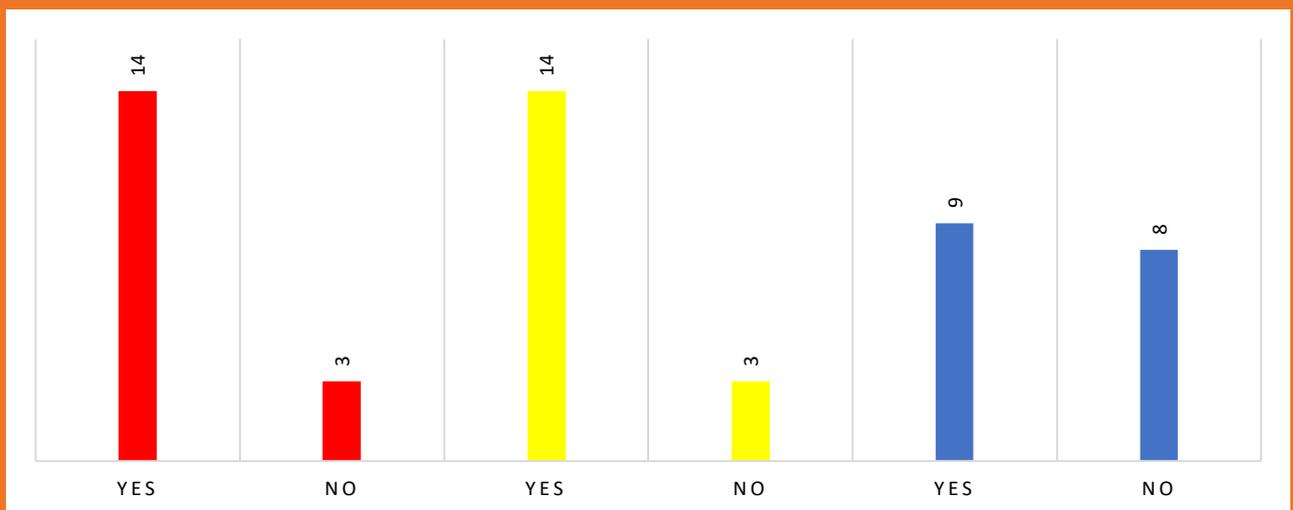


Figure 9. Services available in mobile application

In addition to offering the services mentioned above, the supplier uses digital channels to provide consumers with the most important information related to energy quality, as shown in the next figure.

In most of the member countries (14 out of 17), the suppliers inform their consumers of energy outages through their digital channels. Furthermore, suppliers provide written guidelines and practical advice for consuming and saving energy more efficiently through communication campaigns on their digital channels. In fewer member countries (9 out of 17), the suppliers provide consumers the option to view their consumption online on websites and/or mobile apps.



Information on energy outage provided through digital channels



New home energy saving potentials



View consumer's consumption online on website or mobile app



Figure 10. Additional available information



Smart technologies represent the core of digitalization, especially smart meters that increase the efficiency of the electricity system and provide enough information to the consumers, allowing them to be more active in the market. In addition, small-scale distributed electricity generation enables the consumer to be more independent from the national grid and enhances their participation in the market.

### 3.1. Smart meters

Smart meters are the fundamental component of smart grids, and they're one of the means that allows the digitalization of the energy system.

Smart meters are electronic measurement devices that precisely record the energy consumption data and allow communication between the different nodes of the network.<sup>3</sup>

On the consumers' side, smart meters enable the use of more innovative mechanisms and policies in terms of tariff settings, allowing remote control, including switching between payment modes, permitting users to monitor their consumption, and allowing potential communication with other smart devices at home.

For the operators, it provides more flexibility in terms of network management, facilitates accurate billing, and reduces "non-technical losses."<sup>4</sup>

Many countries in the Mediterranean region already have a high share of consumers equipped with smart meters, mainly in the northern shores of the region (France, Italy, Spain, Montenegro, Malta, and Portugal). On the southern shores, most countries have initiated the implementation of smart meters by launching pilot projects. The below figure provides an overview of the state of implementation of smart meters in the Mediterranean region and the role of NRAs in approving the investments regarding smart meters.

---

<sup>3</sup> See MEDREG's report on "smart grids": [Download the report here.](#)

<sup>4</sup> See MEDREG's report on « Regulatory practices on handling technical and non-technical losses for electricity »: [Download the report here.](#)



Figure 11. Smart meters' state of play in the Mediterranean region<sup>5</sup>

The functions of smart meters can vary depending on the user needs; in the Mediterranean region, the main functions are as follows:<sup>5</sup>

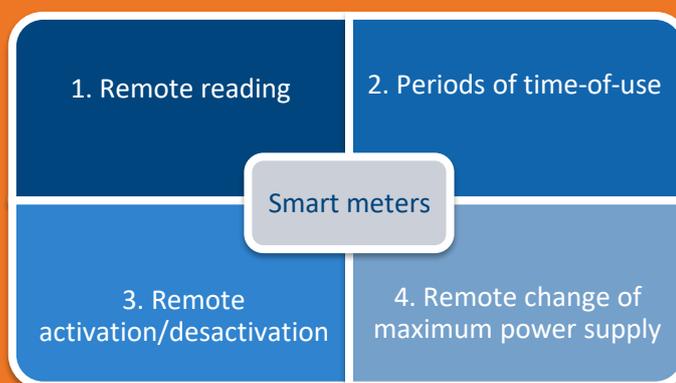


Figure 12. Main functions of smart meters in the Mediterranean region

The first three functions are used in all the countries listed in Figure 11. However, the function of remotely changing the maximum power of supply is used in six countries (out of 9).

<sup>5</sup> In Egypt, GASREG approves the investments regarding smart meters. In Portugal, the government didn't approve the roll-out of smart meters; therefore, ERSE couldn't approve it either. For France, the total objective is to reach 37.4 million by 2021; in summer 2021, the number of smart meters reached 32 million. In Lebanon, 865 net meters are installed, of which 40 meters are smart, and the remaining are digital meters with limited "smart" functionalities.

## 3.2. Distributed electricity generation

As mentioned in the previous sub-chapter, smart meters allow communication between the different nodes of the network, which unlock the potential to use other technologies and mechanisms, meaning consumers can use the functions pertaining to self-consumption and small-scale distributed electricity generation.

The analysis of the legal framework in the Mediterranean region shows that three types of distributed electricity generation are the most used in the region, namely local communities, self-consumption/generation, and prosumers.

Since the beginning of the development of renewable energies, consumers have always demonstrated interest in installing proper renewable energy equipment to produce at least a part of their consumption in return for economic or social/environmental benefits.

In most of the countries in the Mediterranean region, self-consumption/generation and prosumers are defined in the legislation. Furthermore, for the prosumers, incentive mechanisms are in place to promote this category of consumers, either by net metering or net billing.

In some countries, the customer involvement in the energy market is even more important; local energy communities consist of an association of several consumers that create a cooperative to produce their energy. The European Commission recognizes certain categories of energy communities in the legislation. In the Mediterranean region, only some of the north shore countries have a legal definition of “local energy community”; in Portugal, it is defined as “renewable energy community,” and it should be located near a renewable energy project or carry out activities related to the renewable energy projects of the respective energy community and developed by the same energy community. In France, it is defined in the primary legislation in the Ordonnance n° 2021-236 du 3 Mars 2021 and in the secondary legislation in current drafting of an implementing decree, by the French Ministry of Energy and Climate Change (DGEC) with the help of stakeholders. Similarly, in Italy, local energy communities are defined in the Italian primary law (Law-Decree 30 December 2019, n.162), and the secondary legislation: ARERA Deliberation 4 August 2020, 318/2020/R/eel. In Greece, according to Law 4513/2018, energy community is defined as a fully-fledged urban cooperative aiming to promote social and solidarity economy and innovation in the energy sector, address energy poverty, promote energy sustainability as well as energy generation, energy storage and self-consumption, enhance energy self-sufficiency and security of supply in island municipalities, as well as improving the energy efficiency at the local and regional level through its activity in the sectors of renewable energy sources and cogeneration to promote the rational use of energy, energy efficiency, sustainable transport, demand response, and generation management as well as the distribution and supply of energy.

<b>Distributed electricity generation</b>	Self-consumption generation	Legal definition: 12 out of 16
	Prosumers	Legal definition: 7 out of 16 Obligation to apply at NRA level: 2 out of 7 Net metering: 6 out of 7 Net billing: 5 out of 7
	Local energy communities	Legal definition: 4 out of 16. Incentives: 3 out of 16

Figure 13. *The legal framework of distributed electricity generation in the Mediterranean region\**

\* GasReg regulates only gas; therefore, the total number of the analyzed regulators are 16 instead of 17.



The energy sector is experiencing a transformation. Major shifts in the global supply and demand on almost every front are creating both fresh opportunities to explore and new threats to manage. This transition is also being shaped by the digitalization of the industry. The adoption of intelligent, sophisticated technology, including artificial intelligence (AI) for controlling and monitoring systems is enabling new business models and more efficient asset management. The digitalization and the development and transformation of energy supply chains are at the core of many governments and businesses' priorities.<sup>7</sup>

The “digital age” and the development of new digital technologies are bringing rapid changes in the form of connections, integration, supply chain management, models, and much more.

Energy systems comprise both IT infrastructures and electrical systems that include cyber systems, people, physical systems, money, etc. Threats can be physical, internal, or external, and cyber threats can emerge from anywhere. The cybersecurity of critical infrastructure, especially in the energy sector, is becoming more important for the safety and security of energy production, distribution, transmission, and storage, as well as for the stability of the energy market.

Energy infrastructures are complex systems that have physical, geographical, logical, and, finally, cyber interdependencies with other critical infrastructures, e.g., transport, telecommunications, water, agriculture, health, finance, chemical industry, and networks supporting the government, central and territorial entities, emergency services, as well as military and civil defense. A disruption in the normal operation of critical energy infrastructures can have a negative cascading effect on other infrastructures, as well.

With new technologies and digitalization, the resilience of the energy sector is greatly increased because they enable the use of several technologies to detect threats, thereby increasing operational accessibility, productivity, sustainability, and safety. On the other hand, digitalization presents new challenges for energy companies as they can be affected by cyber or digital disruption attacks that can impact every operation within an energy sector.

This report tries to detect the institutional and legislative framework where cyber security issues are faced in different countries in the MEDREG region and to present national strategies (if any) related to the security of network and information systems as well as any other legislation/guidelines/standards related to cyber security in the energy sector.

The following figure summarizes the results of the research conducted in the MEDREG region regarding the existence of national strategies or other relevant documents related to the security of network and information systems and the number of countries having national strategies or other relevant documents on cybersecurity in the energy sector:

---

<sup>7</sup> Cyber challenges to the energy transition, World Energy Council  
([https://www.worldenergy.org/assets/downloads/Cyber\\_Challenges\\_to\\_the\\_Energy\\_Transition\\_WEC\\_MMC\\_2019.pdf](https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC_MMC_2019.pdf))



Figure 14. Existence of national strategy related to the security of energy networks and information systems in MEDREG members countries

According to data provided, 12 countries have a national strategy or law related to the security of network and information systems, three countries don't have any document related to the security of network, and relevant data are not available for two countries.

In Cyprus, there is the "Cybersecurity Strategy of the Republic of Cyprus," which was adopted in June 2020<sup>8</sup>. In Egypt, "The Egyptian National Cybersecurity Strategy 2017–2021" covers issues related to the security of network and information systems.

France has the National Cybersecurity Acceleration Strategy (Stratégie Nationale d'accélération pour la Cybersécurité), which was adopted in February 2021.

The Government of Greece adopted a cybersecurity strategy for the period 2020–2025 in December 2020, taking into consideration the national L. 4577/2018 (Article 6) "Transposition of EU Directive 2016/1148/EE into national legislation, regarding the Network Information Security."

Italy has the "National Plan for Cybernetic Protection and Informatic Security," which was adopted in 2017<sup>9</sup>. Moreover, Italy has Legislative Decree n. 65 from May 2018, which was transposed. Directive 2016/1148/EU

<sup>8</sup> link to strategy: <https://dsa.cy/wp-content/uploads/csarc-2020.pdf> (only in Greek)).

<sup>9</sup> link: <https://www.sicurezza nazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf>

(Network and Information Security Directive). In addition to the above, Italy by Law-decree from June 14, 2021, established the Agency for National Cybersecurity.

The government of Montenegro adopted a cybersecurity strategy for the period 2018–2021 in December 2017. In 2021, it was planned that the government would adopt a cyber security strategy for the period 2022-2026.

In 2019, the Spanish government approved the National Strategy on Cybersecurity by Order PCI/487/2019<sup>10</sup>.

Albania has regulations on the cybersecurity of critical infrastructures in the power sector, and there is also in force a law and government decision on cybersecurity (Law Nr. 2/2017, "On Cybersecurity", Gov decision Nr. 553, date: July 15, 2020, "on critical infrastructures..."). Algeria has a law on the protection of individuals in the processing of personal data from 2018, and in 2020, Algeria established a national system for the security of information systems.

Portugal adopted the "Law on Legal Regime for Cyberspace Security" in 2018 and the National Cyberspace Security Strategy for the period 2019–2023 in 2019. In Turkey, the Presidential Digital Transformation Office Information Security Guide has been available since 2019.

The data gathered through this report suggests that most countries that have adopted a national strategy or law related to the security of network and information systems also cover the energy sector with these documents. Ten countries have their energy systems included in the national strategy or a law related to the security of network and information systems, five countries don't include energy systems in their strategy, and relevant data are not available for two countries.

The results of the conducted research show that most countries have more than one national competent authority designated to monitor/coordinate the implementation of the strategy, the action plan (if applicable), and other legislation related to the security of networks and information systems, except for Lebanon and Malta.

According to the data provided, 12 countries have one or more national competent authorities designated to monitor/coordinate the implementation of the strategy, the action plan, and other legislation related to the security of network and information systems, two countries don't have any relevant authority, and for three countries, the data are not available. The detailed results are provided by country in the annex.

Cybersecurity standards are collections of best practices, created by experts to protect organizations from cyber threats. Cybersecurity standards and frameworks are generally applicable to all organizations, regardless of their size, industry, or sector. Through this report, we try to determine whether there are any national or adopted international information and cybersecurity-related standards. According to the data provided, nine countries have national or adopted international information and cybersecurity-related standards, three have no pertinent standards, and for five countries, the data were unavailable.

The specific details related to the cybersecurity standards from country to country is listed in the annex.

---

<sup>10</sup> link: <https://www.dsn.gob.es/es/file/2989/download?token=EuVy2INr>



In this report, we analyze the role of digitalization and its impact on consumer issues in the Mediterranean region from a regulatory point of view. From surveys, we found out that digital channels and services are available at the regulators', distributors' (DSOs), and supplier's levels.

The communication and availability of information at the regulators' level are crucial in raising consumer awareness regarding their obligations and rights, as well as their role in the energy systems. In the observed countries, most regulators share general information (customer corner), information related to the consumers' rights and tariffs, and information related to energy-saving, using at least one social media application. This may lead to well-oriented/informed consumers who can contribute to the energy transition in a more efficient way. At the DSO level, the availability of information and transparency are critical issues. Across the Mediterranean region, DSOs use at least one communication channel and facilitate access to services and information by making them available online, like grid connection information and process, relevant data such as that on consumption, communication in case of disturbance or outages, and the availability of online support.

To increase consumers' awareness, it is important that suppliers offer public information that is easily available, accessible, and understandable by all consumers. In the MEDREG region, suppliers offer the following online services to consumers: bill calculator, complaint management tools, online payment, consumption history, information on energy savings, meter reading submission applications, and other tools. To facilitate the participation of consumers in the market, it is important to have clear and simple procedures, transparency of information, and online services. Also, it is advisable to have a single point of contact to provide consumers with all the necessary information concerning their rights and current legislation.

Smart technologies represent the core of digitalization, especially the smart meters that represent the first step toward the digitalization of the energy system. They provide more and accurate information to operate the electricity and gas systems in an efficient way while reducing the costs. Furthermore, they provide enough information to the consumers that allows them to be more active in the market. In addition, small-scale distributed electricity enables the consumer to be more independent from the national grid and enhances their participation in the market. In the MEDREG region, cooperation between north and south shore countries may help boost and foster the implementation of smart meters in the south shore countries.

Besides the digitalization of the energy system, an attempt to benchmark the current state of cyber security in the energy system was developed in this report.

Digitalization presents new challenges for energy companies as they can be affected by cyber or digital disruption attacks that can impact every operation within an energy sector. It is thus highly recommended to start a discussion among the regulators on how to develop and adopt new legislation and standard to reinforce cyber security in energy, in addition to the general cyber laws, to tackle the digital threats to the energy systems.

# ANNEXES

## Annex 1: National competent authorities designated to monitor/coordinate the implementation of the strategy

In **Albania**, the regulator (ERE) has approved the regulation on the cyber security of critical infrastructures in the power sector. The purpose of this regulation is to define the rules and measures that shall be taken by the entities licensed by ERE in the power sector, responsible for guaranteeing cybersecurity in critical infrastructures that they own and operate. Measures concerning cybersecurity in the power system ensure the uninterrupted supply of electricity for the consumers in Albania.

In **Algeria**, the National Council for the Security of Information Systems and Information Systems Security Agency are designated to follow up on the implementation of the strategy and other legislation related to the security of network and information systems.

In 2018, the legislation on the Security of Networks and Information Systems was introduced in the **Republic of Cyprus**, based on which the Digital Security Authority was established under the Communications Commissioner, the implementation of the Network and Information Security Directive (NIS Directive) and the coordination of actions for the implementation of the National Cybersecurity Strategy, which includes the operation of the National CSIRT. The competent authority to monitor the energy sector is the Ministry of Energy, Commerce, and Industry.

In **Egypt**, the Egyptian Supreme Cybersecurity Council develops a national strategy to face and respond to cyber threats and attacks and oversees its implementation and update.

In **France**, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) is designated for monitoring/coordinating the implementation of the strategy and other legislation related to the security of network and information systems, and in **Greece**, the Ministry of Digital Policy, specifically the National Cybersecurity Authority of the General Directorate, is the competent authority for the implementation of the national strategy for all critical infrastructures. For the energy sector specifically and depending on the case, the Ministry of Environment Physical Planning & Public Works, Regulatory Authority for Energy, and Hellenic Centre for Security Studies, are also involved.

A Law-decree from 2021 establishes the Agency for National Cybersecurity in **Italy**. At present, the Ministry for Economic Development is entitled to the National Institute of Standards and Technology (NIST) cybersecurity framework in the energy sector.

The Ministry of Capital Investments is the competent authority for the energy sector in **Montenegro**, and in **Portugal**, there is a national entity called the National Cybersecurity Centre. The National Cybersecurity Centre is the operational coordinator, and the Portuguese national authority specialized in cybersecurity works in this field with state entities, operators of critical infrastructures, operators of essential services, and digital service providers, ensuring that cyberspace is used as an area of freedom, security, and justice for the protection of all the sectors of society that come under national sovereignty and the democratic state under the rule of law.

According to the national strategy in **Spain**, there are three authorities in charge of cybersecurity matters: the National Security Council, the National Cybersecurity Council, and the Specialized Situation Committee.

This governance structure is completed with the Standing Committee on Cybersecurity that ensures inter-ministerial coordination at an operational level.

In **Turkey**, the regulator (EMRA) has the authority to supervise the provisions of "Information Security Regulations in Industrial Control Systems used in the Energy Sector" and "Safety Analysis and Test Procedures and Principles for Industrial Control Systems used in the Energy Sector," following the task assigned to it within the framework of being the "Industrial Cyber Incidents Response Team."

## Annex 2: Cybersecurity standards

- **Albania:** Critical infrastructure operators in the electricity sector are required to provide certification with the safety standard ISO 27001.
- **Algeria:** ISO / IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements; ISO / IEC 27002:2013 (Information technology — Security techniques — Code of practice for information security controls); ISO/IEC 27035:2016 (Information technology — Security techniques — Information security incident management), and GDPR 2016 (General Data Protection Regulation UE)
- **Cyprus:** European standards on cyber security have been adopted as the national standard.
- **Egypt:** Standards are being developed by the Egyptian Supreme Cybersecurity Council.
- **France:** 1. A draft of European Framework Guidelines (FG) for a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting, and crisis management, was elaborated by the Agency for the Cooperation of Energy Regulators (ACER) on July 6, 2021, in response to a request from the European Commission earlier in the year, in the application of Article 59(4) of Electricity Market Regulation of 2019. The network code shall be submitted to the European Commission for approval before it becomes effective. 2. The Network and Information System Security (NIS) Directive, under its official name Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016, on measures to ensure a common high level of security of networks and information systems in the Union, is currently under revision. Before coming into effect, it must be negotiated between the three European institutions (Parliament, Council of the EU, and European Commission) and then transposed in national legislations.
- **Italy:** The EU Agency for Cybersecurity "ENISA"<sup>11</sup> has published a series of safety standards valid at the European level.
- **Lebanon:** A lot of standards have been implemented in the sector of information technology, and these standards are adopted as national standards; however, these standards are not only used for the energy sector.
- **Malta:** DSO information and cybersecurity-related standards are guided by ISO27001 principles.

<sup>11</sup> <https://www.enisa.europa.eu/>



Co-funded by  
the European Union

**MEDREG – Association of Mediterranean Energy Regulators**  
Via Fieno 3, 20123 Milan, Italy –Tel: +39 3402938023  
[info@medreg-regulators.org](mailto:info@medreg-regulators.org) [www.medreg-regulators.org](http://www.medreg-regulators.org)