2025 ECRB REPORT

REMIT Data Protection Standards of NRA

December
2025

Table of Contents

INTRODUCTION

1. About ECRB

The Energy Community[1], established by the Treaty signed in 2005, under which Contracting Parties committed to implementing core elements of the EU energy acquis, including electricity, gas, renewables, energy efficiency, and market integrity frameworks.

Within the institutional structure of the Energy Community, the Energy Community Regulatory Board (ECRB) serves as the platform for cooperation among national energy regulators of the Contracting Parties and Observers. The ECRB facilitates coordination with EU regulators, supports implementation of the acquis, and issues recommendations and reports to strengthen regulatory practices. Its work builds on the principle that regional regulatory cooperation is essential for competitive, secure, and transparent energy markets.

The ECRB operates through specialised Working Groups and Task Forces, including the REMIT Working Group (WG), which coordinates activities related to the Regulation on Wholesale Energy Market Integrity and Transparency. This report was prepared by the ECRB REMIT WG, within the Task Force Cybersecurity and Data Protection Standards led by Mr Alija Mujcinagic (SERC, Bosnia and Herzegovina). The active participation and inputs of all Energy Community Regulatory Authorities were vital to the successful completion of this work.

2. Background

The EU's Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT) was adopted in 2011 to prevent market abuse, strengthen oversight, and ensure consumer confidence in fair energy pricing. In the EU, REMIT is enforced through the Agency for the Cooperation of Energy Regulators (ACER), which collects market data, monitors trading behaviour, and coordinates cross-border investigations.

Recognising the absence of such a framework in the Contracting Parties, the Energy Community Ministerial Council adopted REMIT for the Energy Community in 2018 (Decision D/2018/10/MC-EnC). This version, known as EnC REMIT, adapts the core provisions of EU REMIT to the regional context. It prohibits insider trading and market manipulation, introduces obligations to publish inside information, and empowers NRAs to investigate and sanction abuses. Unlike in the EU, EnC REMIT does not foresee

[1] www.energy-community.org.The Energy Community comprises the EU and Albania, Bosnia and Herzegovina, North Macedonia, Georgia, Kosovo*, Moldova, Montenegro, Serbia and Ukraine. Armenia, Türkiye and Norway are Observer Countries. Throughout this document the symbol * refers to the following statement: This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Advisory Opinion on the Kosovo declaration of independence.

centralised data collection by ACER, but instead relies on national regulators and coordination within ECRB to ensure consistent enforcement.

Since its adoption, EnC REMIT has become the cornerstone of the market integrity framework in the Contracting Parties. The ECRB supports its implementation through guidance, procedural acts, and coordination of cross-border investigations.

3. Objective of this report

In light of growing need for NRAs to collect and assess market sensitive data and information, the ECRB REMIT Working Group launched a dedicated Task Force on Cybersecurity and Data Protection. Its objective is to assess how Contracting Parties' NRAs protect sensitive REMIT-related data, evaluate preparedness for alignment with ACER standards, and identify capacity-building needs.

This report presents the findings of the survey of NRAs, combining quantitative responses and qualitative feedback.

4. Methodology

A standardised questionnaire covering six overall themes was drafted and shared with NRAs, member of ECRB:

- Roles and responsibilities (dedicated staff, cybersecurity functions, access rights)
- Internal rules and procedures (policies, incident response)
- Legal and regulatory framework (sector-specific laws, reporting obligations)
- Systems and technical measures (collection tools, IT safeguards)
- Staff training and monitoring
- Challenges and support needs

The questionnaire was circulated in spring 2025. Responses and input were received from ERE (Albania), REGAGEN (Montenegro), AERS (Serbia), ERC (North Macedonia), ANRE (Moldova), GNERC (Georgia) and NEURC (Ukraine), SERC (Bosnia and Herzegovina) and ERO (Kosovo*).

In addition to the tick-box replies, several NRAs provided detailed written explanations. These have been integrated into the analysis to illustrate practices and highlight legal and institutional arrangements.

FINDINGS

1. Roles and Responsibilities

Most NRAs do not yet have a dedicated team for protecting REMIT-related data. Responsibilities are often integrated into existing legal or IT departments. For example, at ANRE REMIT data protection tasks are handled within its Licensing section, with responsibilities embedded in the unit's functional duties.

Cybersecurity functions are more developed: NRAs in Serbia, North Macedonia, Moldova, Georgia, Montenegro, Albania, Kosovo* and Bosnia and Herzegovina have IT or security staff responsible for protecting systems from cyberattacks. NEURC (Ukraine) has not yet finalised such arrangements.

Access to REMIT sensitive market data and information is generally restricted to staff directly involved in REMIT monitoring and enforcement. NRAs that do not receive sensitive data on regular basis do not apply such restriction.

2. Internal Rules and Procedures

There are many divergences regarding internal procedures across NRAs. AERS and ANRE have adopted comprehensive rulebooks: AERS referred to its Internal Rulebook on Data Protection and Internal Rulebook on Cybersecurity, both based on national laws. ANRE has a general internal regulation on information security that applies across the agency, including to REMIT data.

ERC, ERO, GNERC and SERC are still developing their internal procedures. ERC highlighted that it adopted a Rulebook on Market Monitoring in 2023 and has prescribed confidentiality requirements, while an internal act on data storage and access exists but needs updating. GNERC reported that its Incident Response Policy and Incident Management process had been drafted but was not yet in force.

Incident response planning is present in ANRE and ERC. REGAGEN and SERC, by contrast, reported no written plan, while AERS acknowledged the absence of a specific breach procedure. ERE and GNERC are planning to instal an incident response plan.

3. Legal and Regulatory Framework

Several Contracting Parties have recently advanced their legal frameworks regarding data protection and cybersecurity. Below represents a state of play:

- Bosnia and Herzegovina: SERC reported that the new legal framework, after several years of preparation, is still under the adoption procedure. The law provides the basis for developing an

organized electricity market in BiH, as well as for transposing the key elements of the Risk Preparedness Regulation.

- Georgia: applies the Information Security Law, mandating ISO or NIST standards across all sectors. Additional energy-specific regulations are under preparation.
- Kosovo*: applies its national cybersecurity framework and requires that cybersecurity incidents be reported to the National Cybersecurity Agency (AKISH) and to the Information and Privacy Agency (IPA) when breaches involve personal or market-sensitive data.
- Moldova: adopted Law No. 48/2023 on Cybersecurity, creating a national framework and assigning incident reporting to the national Information Technology and Cybersecurity Service (STISC).
- Montenegro: REGAGEN relies on Article 18 of its REMIT Law, which obliges the regulator to protect market data during investigations. Law on Information Security sets the broader sector-specific cyber framework. It sets cybersecurity obligations for key entities, including compliance with information security management standards MEST ISO/IEC 27001.
- North Macedonia: introduced ISO 27001 standards and in 2023 adopted Rules on Cybersecurity under the Energy Law. In 2025, a National Council for Digital Transformation and Cybersecurity was established.
- Serbia: applies the Law on Cybersecurity (2016, amended 2019) and detailed by-laws. AERS adopted a Rulebook on Cybersecurity accordingly, with incidents reported to the national CERT (RATEL).
- Ukraine: NEURC reported no dedicated legal requirements for the energy sector.

4. System and Technical Measures

The technical landscape is also very diverse among NRAs:

- SERC currently handles documentation mostly manually and relies on basic IT protections security tools but does not yet have a dedicated REMIT data platform.
- GNERC collects transaction reports via API connections and restricts access to certain staff. It plans to introduce multifactor authentication in the near future.
- ANRE uses general IT protections (passwords, firewalls, restricted access), but does not yet operate a dedicated REMIT data platform.
- ERC operates a special Market Monitoring platform through which license holders report on templates across energy sectors. The platform, however, does not yet cover REMIT data. The NRA also approved cybersecurity investments for license holders (operators), introduced the C2M2 model as a reference framework, and required companies to self-evaluate readiness.
- REGAGEN, ERO and ERE also rely on basic IT measures and email-based processes.
- AERS still processes documentation largely manually, though it has partially automated market participant registration. Protections are limited to passwords and antivirus software.
- NEURC reported that no systems are currently established.

5. Staff training and Monitoring

Structured training related to data protection is largely absent across NRAs from the Contracting Parties. ANRE, AERS, ERC, ERO, REGAGEN, NEURC and SERC reported no specific training for staff handling REMIT-related data. GNERC indicated that general cybersecurity training had been conducted and further sessions were planned. ERE also noted training as a planned measure.

6. Main challenges

NRAs face obstacles in handling data and information in the context of data protection, Among the most common obstacles mentioned by the NRAs are:

- Lack of specialised staff (AERS, ANRE, GNERC, NEURC, REGAGEN, SERC, ERO).
- Limited financial resources (ERC, GNERC, NEURC, REGAGEN, ERO).
- No clear procedures/tools (AERS, ANRE, REGAGEN, SERC).
- Unclear legal framework (ERE, REGAGEN, SERC).

In addition, ERC stressed the need to learn from other NRAs and establish structured cooperation with the national electricity market operator.

7. Support Needed

NRAs lack resources to ensure high standards for data and information protection. They highlight the need to support in the following:

- Technical training for staff.
- Regional workshops to exchange experience.
- Assistance in drafting procedures.
- Shared IT tools or platforms.
- Guidelines based on ACER and EU practices.

8. ACER Standards

ACER overarching Information Security Management System is based on ISO 27001. In addition, the REMIT Information Security Framework is aligned with ISO 27002 and the EU Cybersecurity Regulation.

EnC NRAs are not fully aware on the details of standards applicable by ACER regarding data protection and cybersecurity. ACER's standards and policies would be an important benchmark for NRAs in this regard, therefore applying such standards should be an objective.

9. Planned Improvements

Planned reforms reflect varying stages of readiness of NRA, taking into account also regulatory and market developments:

- ERC, and ERO noted the need to strengthen oversight, education and capacity building, and developing the regulatory framework.
- GNERC stated the need for improvements in line with the developing sector-specific regulations and implementing ISO/NIST standards.
- ANRE and NEURC emphasised strengthening oversight and capacity building.
- REGAGEN and ERE are planning capacity-building activities.
- AERS noted that improvements dependent on primary legislative changes.
- SERC highlighted its efforts in planning capacity-building activities, noting that the introduction of an automated process for data collection and processing remains dependent on primary legislative changes.

CONCLUSIONS AND RECOMMENDATIONS

The input provided by NRAs reveals a fragmented picture of cybersecurity and data protection applicable by NRAs in the Contracting Parties:

- There is work by few NRAs in progress to advance the frameworks through establishment of legal obligations, platforms, and oversight tools.
- Few NRAs are at the early stage of development. They have minimal arrangements and depend heavily on general law.
- Few NRAs have dedicated REMIT staff, incident response plans, or advanced IT safeguards.
- Most NRAs lack structured capacity-building for staff emphasising the training gaps.
- There is a strong demand for cooperation by all NRAs, primarily in the context of guidance, shared tools, and workshops based on ACER/EU practice.

NRAs should ensure that sensitive data and information provided to them by market participants are kept safe and protected based on best available standard. Dedicated resources in this regard are necessary to achieve such standards.

The ECRB outlines the following recommendations for NRAs:

1. Develop dedicated policies (aiming ACER's standards) and teams for REMIT data protection.
2. Adopt incident response plans aligned with EU best practices.
3. Strengthen IT measures, including encryption, multifactor authentication and secure transfer protocols.
4. Launch training programmes for staff handling market data.
5. Close legal gaps, especially in countries without sector-specific cybersecurity frameworks.
6. Enhance regional cooperation under ECRB, including joint workshops and IT tool development.
7. Promote peer review and audits to benchmark practices across NRAs.

ECRB will continue to work with NRAs to strengthen cooperation, coordination, and the exchange of experience and knowledge among them, including with NRAs from EU Member States and ACER. Furthermore, ECRB calls on the Energy Community Secretariat to support NRAs by facilitating the adoption of European and ACER practices on REMIT data management and cybersecurity, including through dedicated workshops, gap analyses and expert assessments.