



Global Compliance News



Moldova



Accession to EU - CE Marking Acceptance

The Republic of Moldova and the European Union have initiated the negotiation process for accession to the European Community. As a result of the negotiations amendments were made to the Law 235/2011 regarding accreditation and product certification. The amendments were published in the Official Journal of Republic of Moldova Nr 448-451 on 28.08.2025 and enter into force on 28.02.2026.

What does this alignment mean for product certification in Moldova?

The Moldovan govt now recognizes CE Marked products. If a product is in full compliance with EU CE marking regulations, the products will now be permitted to be sold and used in Moldova without any further certification activity.

Previously, products were required to comply with Moldovan regulations, which typically involved testing against national standards. However, under a new cooperation agreement with the Moldovan regulator, radio equipment and other electrical and electronic devices that have already undergone conformity assessment in accordance with the relevant EU directives—are fully compliant, bear the CE marking, and are accompanied by an EU Declaration of Conformity—can now be placed on the Moldovan market without the need for any additional conformity assessment or certification.

Australia Updates Low Interference Potential Devices Regulation



Australia's Radiocommunications Act 1992 has recently introduced a crucial update: the Radiocommunications (Low Interference Potential Devices) Class Licence 2025, effective 1 October 2025. This class licence simplifies spectrum access for many low-power wireless devices. Instead of applying individually, compliant devices can operate freely within designated conditions.

What Are LIPD Devices?

Low Interference Potential Devices (LIPD) are short-range, low-power transmitters that share spectrum bands with minimal disruption. These include Wi-Fi, Bluetooth, RFID readers, remote controls, wireless microphones, and radar systems.

These devices previously operated under the 2015 class licence. With the release of the 2025 version, those conditions are refreshed and spectrum access is broadened.

Key Changes in the 2025 LIPD Licence

The updated licence introduces new frequency bands, updated terminology, and reorganized transmitter categories. Notable additions include support for Wireless Multi-Channel Audio Systems (WMAS) in the 520–694 MHz range and radiodetermination devices in the 13.4–14 GHz and 76–77 GHz bands. Moreover, the licence adds new conditions for RLAN transmitters in the 6425–6585 MHz band.

Technical and Compliance Requirements

Compliant devices must operate within defined EIRP and bandwidth limits. Depending on the device, features like frequency hopping or adaptive power control may be required. Furthermore, manufacturers need to follow applicable labelling and EMC standards under the equipment rules. It's important to note that LIPD devices cannot claim protection from interference. They must accept potential disruptions from other compliant users in the same band.

Australia Cyber Security Rules 2025

The new Australian Cyber Security (Security Standards for Smart Devices) Rules 2025 will take effect on 4 March 2026. The rules will apply to any relevant connectable product – this is defined in two ways:

- Internet-connectable product, i.e. any device that directly connects to the internet using the internet protocol suite (TCP/IP, UDP, IP).
-

For example: routers, switches, IP cameras, VoIP phones.

- Network-connectable product, i.e. any device that connects and communicates directly to an Internet-connectable product but doesn't connect to the internet on its own.

For example: Bluetooth speakers and headphones.

However, some items will be exempt from the rules:

- Desktop or laptop PCs.
- Smartphones and tablets.
- Medical devices covered by the Therapeutic Goods Act.
- Vehicle and vehicle components covered by the Road Vehicle Standards Act.

Australia Cyber Security Cntd..

What's Required?

The Rules contains four main components:

- 1.Any pre-defined password is unique and not easily guessable.
- 2.Security issues (related to hardware and software) can be reported to the manufacturer.
- 3.The manufacturer must publish the defined support period for the product. While no minimum support period is defined, the support period cannot be shortened after publication.
- 4.A Statement of Compliance must be prepared or signed by the manufacturer (or authorised representative) and kept on file.

Relationship to European Regulations

The Australian Rules have been taken in part from the EU standard EN 303 645, which contains 13 provisions for cyber security and 5 for data protection. A device compliant with EN 303 645 will already meet most of the Australian requirements. You will still need to prepare and file a Statement of Compliance.

The Rules will apply to all products for sale on or after 4 March 2026. The Australian government has granted one year from the publication of the Rules for businesses to ensure their product will be compliant.



Jordan Equipment Certification – Updates to Regulations



The Jordan regulator Telecommunications Regulatory Commission 'TRC' published the updated equipment certification rules No. 2 of 2025, which replace the 2024 guidelines on the import and certification of telecommunications and terminal equipment.

Main Updates include:

Changes affecting approval validity – Now Fixed to 2 years

Regulated technologies

Import permissions under specific circumstances such as research or personal use.

New exemption categories such as:

- Desktop computers, printers, and scanners
- Bluetooth-only devices
- Satellite receivers
- Wired landline phones (without radio functions)

Spotlight on Compliance

One of the key questions we are asked by our partners is can product certificates be issued in the name of the manufacturer, or does a local company have to be used as the named certificate holder. Where possible ICM's strategy is to have certificates issued in the name of the manufacturer.

Where this is not possible ICM has our own network of local partners who can provide certificate holding services. Throughout the years we have come across the situation where a manufacturers importer obtained a local equipment certificate, however the local importer would not give any other 3rd party importer a copy of the certificate. So the manufacturer is held hostage by an importer.

The advantage of using ICM's local partners is that issued equipment certificates will be given to all our partners importers, eliminating this risk. An example of our local representative service can be found below:

Algeria	Australia	Brazil	Ghana
Indonesia	Israel	Jordan	Kazakhstan
Lebanon	Malaysia	Mexico	Serbia
Singapore	South Africa	Thailand	Vietnam