Stay Ahead of EU Regulatory Changes with Tosibox: Future-Ready and Secure

We, at Tosibox, are ready for the RED Cybersecurity directive.

The European Union's Radio Equipment Directive (**RED**) 2014/53/EU provides a regulatory framework for introducing radio equipment to the market. Its primary goal is to ensure safety, health, electromagnetic compatibility, and efficient use of the radio spectrum.

From 1 August 2025, all wireless devices sold in the EU must comply with new harmonised information security requirements, which will become part of the CE marking process.

How Tosibox Meets and Exceeds EU Security Standards

We are committed to delivering the highest level of security. Our Tosibox Nodes and Key hardware tokens are already CE marked and not only meet but exceed these upcoming stringent security regulations.

We are certified with ISO27001 and ISO9001. In both, a lot overlaps with the RED directive. ISO 27001 is the worldwide known standard on how to manage information security. It lays out requirements for establishing, implementing, maintaining, and continually improving information security management system (ISMS).

ISO9001 is the international standard that specifies requirements for a quality management system (QMS). The ISO 9001 certification stands out as the essential part of Tosibox Quality Management Systems and defines the basis for Tosibox´s High Quality Policy.

Tosibox is built on secure-by-design principles, ensuring that our devices offer robust protection against modern cybersecurity threats while meeting all upcoming regulatory requirements.

1. Data Privacy Protection

At Tosibox, we prioritize privacy and security. Our devices do not collect or store personal data or any information that could jeopardize customer privacy. We collect and process only the data necessary to provide our services and maintain system operations, ensuring minimal data exposure.

2. End-to-End Encryption

Security is at the heart of our design. Data transmitted between Tosibox devices, users, and servers is protected with end-to-end encryption, ensuring that the data is encrypted throughout its journey across the network. Strong encryption significantly reduces the risk of interception by unauthorized parties and guarantees secure communication.

3. Built-In Firewall & Security Configuration

Tosibox products come with built-in firewalls and pre-configured security settings to prevent unauthorized access and safeguard your devices and networks from potential attacks. These default security measures are designed to minimize the risk of network harm and ensure resources are protected from misuse.

4. Reliable Connectivity & Troubleshooting

Tosibox offers multiple built-in features to ensure reliable connectivity and quick troubleshooting. Whether it's ensuring smooth operations or resolving issues promptly, our products are designed to minimize downtime and maximize productivity.

Going Beyond Compliance: Tosibox's Commitment to Secure Development

While the security features of Tosibox products contribute significantly to meeting the requirements of the Radio Equipment Directive (RED), compliance also relies on how these features are implemented. At Tosibox, we take a comprehensive approach to security and compliance:

- **Software Development Lifecycle (SDLC)**: Tosibox has a well-defined SDLC in place, ensuring that security is considered at every stage of the development process. Our commitment to security starts from the initial design phase and continues throughout the product lifecycle.
- **Secure-by-Default Configuration:** Tosibox products are configured with secure settings by default, reducing the risk of human error or misconfiguration. This ensures that even when deployed, our devices maintain the highest level of security.
- **Comprehensive Documentation & Support:** We provide detailed documentation, product-specific datasheets, user manuals, and support via our Helpdesk to ensure our customers can easily configure and manage their devices securely.
- **Regular Firmware Updates:** Tosibox provides regular firmware updates to address any newly discovered vulnerabilities or issues. This proactive approach ensures that our devices are always protected against evolving threats.
- **Rigorous Testing & Quality Assurance:** Every Tosibox product update and release undergoes rigorous testing under various conditions to ensure it operates within safe and acceptable parameters, maintaining compliance and security at all times.
- **Regular Security Audits:** We conduct regular security audits on our processes and products to continuously evaluate and improve our security posture. These audits ensure that we stay ahead of potential threats and maintain compliance with the latest security standards