Cybersecurity for lighting & domestic components

How to become well prepared for cyber attacks

In today's increasingly digitized world, cybersecurity is a critical topic. Smart home lighting is increasingly interconnected with other devices through Bluetooth, Wi-Fi, Zigbee, Thread or 4G/5G radio connections. Street lighting is becoming part of smart city infrastructures. EV chargers integrated into luminaires may use wireless communication and digital payment solutions. These developments increase the potential attack surface. Unauthorized access, data leakage, fraud, or disruption of network functionality are real risks. Many manufacturers are still not structurally prepared for these cybersecurity challenges.

To address this, the European Commission activated the cybersecurity requirements under the Radio Equipment Directive (RED) through the RED Delegated Regulation (EU) 2022/30. Since **1 August 2025**, applicable connected lighting products and other radio-enabled domestic components must comply with mandatory cybersecurity requirements before being placed on the EU market.

DEKRA thoroughly assesses **cybersecurity**

At DEKRA, we assess cybersecurity compliance independently and objectively. Our experts support manufacturers in obtaining certificates and seals that demonstrate independent third-party evaluation. With a DEKRA certificate or seal, you strengthen trust in your products and demonstrate compliance with European legislation.

We determine whether your products comply with applicable regulatory and technical requirements by assessing them against:

- **EN 18031 series** (harmonised standards under RED for cybersecurity)
- **ETSI EN 303 645** (consumer IoT baseline)
- **IEC 62443** series (industrial and infrastructure systems)

The benefits of **cybersecurity certification**

- Protect confidential data against cyberattacks
- Protect your customers from cyber incidents affecting your products
- Demonstrate compliance with European legislation (RED and upcoming CRA)
- Reduce liability and product risk exposure
- Strengthen your competitive position in tenders and smart city projects
- Gain independent third-party insight into your cybersecurity maturity
- Show that your organization has structurally reduced cybersecurity risks

RED directive
cybersecurity of products

The RED Delegated Regulation (EU) 2022/30 is European legislation supplementing the Radio Equipment Directive (2014/53/EU). It activates the cybersecurity requirements of Article 3.3 (d), (e) and (f). DEKRA is a Notified Body under the RED Directive, including the cybersecurity requirements of Article 3.3. The RED Directive sets cybersecurity requirements for applicable radio equipment. From 1 August 2025, relevant radio equipment with internet connectivity or data processing functionality must comply with Articles 3.3(d), (e) and (f). These articles include the following:

Article 3.3(d): Network Security:
Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.

Article 3.3(e): security of personal data and privacy:
Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.

Article 3.3(f): protection against fraud:
Radio equipment supports certain features ensuring protection from fraud.

ETSI EN 303 645, EN 18031 and IEC 62443

DEKRA is a Notified Body under the RED Directive, including the cybersecurity requirements of Article 3.3. We determine whether your product is compliant by assessing it against recognised standards, including:

EN 18031 – harmonised standards under RED:
EN 18031-1, -2 and -3 provide presumption of conformity with the RED cybersecurity requirements for applicable radio equipment.

ETSI EN 303 645 for consumer IoT (internet of things) products:
Cybersecurity standard created by the European Standards Organization. ETSI EN303 645 is a standard for cybersecurity in the Internet of Things (IoT) that establishes a security baseline (security and privacy) applicable to all consumer IoT devices.

IEC 62443 for IoT products for industries:
IEC-62443 is a series of standards including technical reports to secure Industrial Automation and Control Systems (IACS). It provides a systematic and practical approach to cybersecurity for industrial systems. Every stage and aspect of industrial cybersecurity is covered, from risk assessment through operations. We have accreditation from IECEE to issue CB certificates for IEC 62443-4-1, IEC 62443-4-2, IEC 62443-3- and IEC 62443-2-4.

Why you should choose DEKRA as your **cyber security testing partner**

- We are an experienced cybersecurity partner. With our expertise of cybersecurity in lighting and domestic components we offer more cyber safety for the products of a whole range of manufactures.
- With a certificate from DEKRA, you give your customers more confidence and strengthen your position in the market.
- We have accreditation from IECEE to issue CB certificates for IEC 62443-4-1, IEC 62443-4-2, IEC 62443-3- and IEC 62443-2-4.
- We have a DEKRA Seal for IEC 62443-4-1. This involves auditing you annually, allowing you to rise in maturity level

Contact us for more information
Scan the QR code to visit our website or contact us via:
sales.nl@dekra.com
+31 88 968 3560