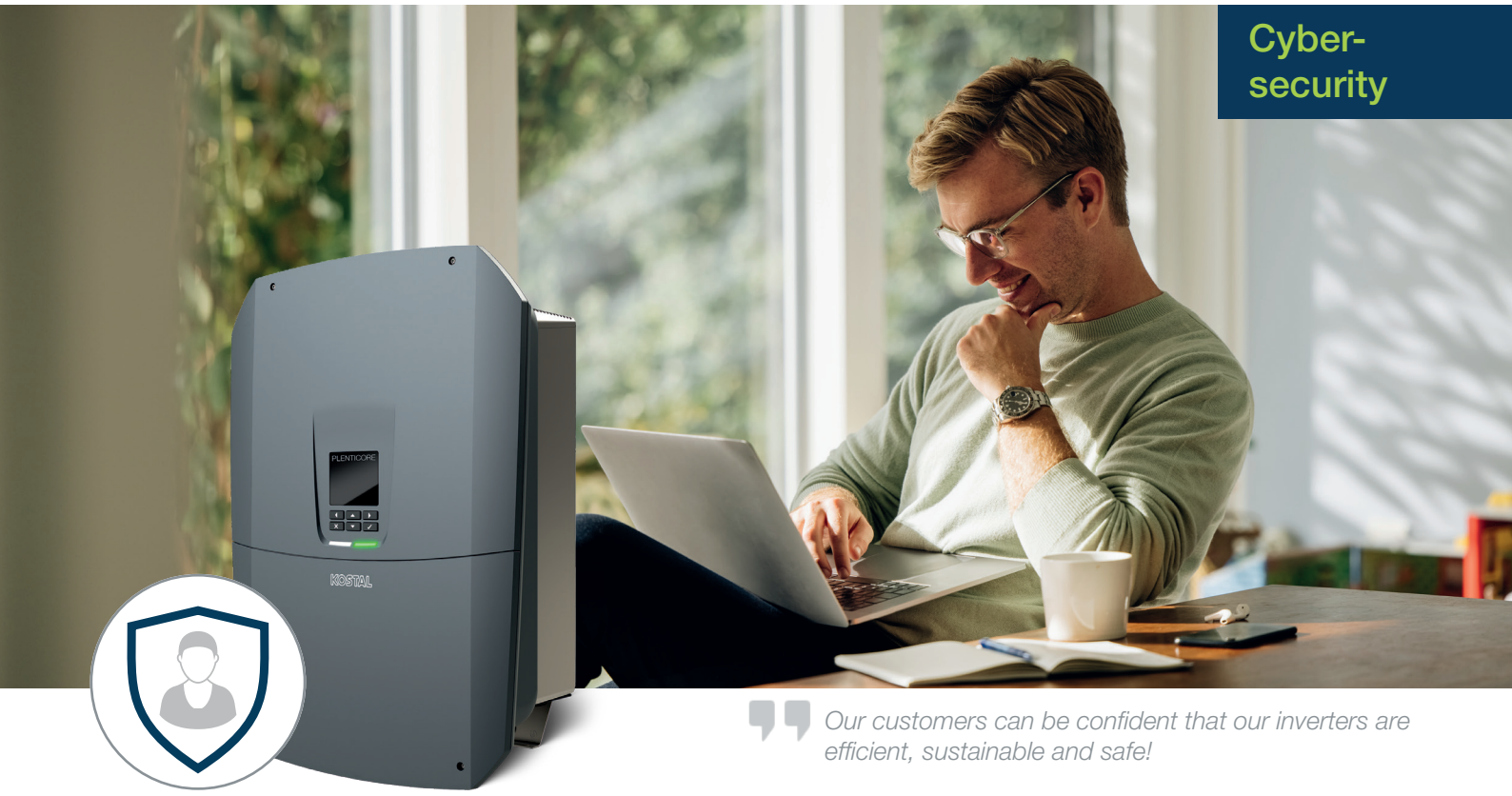
KOSTAL



Our customers can be confident that our inverters are efficient, sustainable and safe!

Cybersecurity at KOSTAL: Highest security standards for a networked future

KOSTAL sets a strong example in cybersecurity for its PLENTICORE inverters and the Wallbox ENECTOR. KOSTAL uses advanced technology and processes to ensure the protection of its products and its customers‘ data. In addition, KOSTAL takes a holistic approach to protect both the devices and the underlying systems and processes against potential threats.

- **Cybersecurity as a corporate:** KOSTAL regards cyber security as a central, company-wide concern that permeates all processes and departments.
- **Technological security measures:** Encrypted communication, personalized access controls and an automated update system ensure the highest security for the inverters.
- **Sustainability & safety combined:** KOSTAL combines efficient energy technologies with robust safety measures for a sustainable and protected energy supply.
- **Proactive security strategy:** KOSTAL sees cybersecurity not only as a reaction to threats, but also as a long-term promise to customers and partners.
- **Trust as a basis:** KOSTAL‘s commitment to safety strengthens trust in the products and supports a safe, networked energy future.

Cybersecurity for our customers

Data protection: Sensitive data is secured by encrypted communication.

Protection against unauthorized access: No one but the authorized user can access the KOSTAL devices.

System stability: Automatic software updates close any potential security gaps (AutoUpdate function).

Trust: Customers do not have to worry about their energy supply.

A strong commitment to safety.

Version EN 01-2025. Subject to change without notice.

KOSTAL is taking comprehensive measures to prove that cyber security is a company-wide concern.

A strong commitment to safety

As a German supplier of inverters and wallboxes, KOSTAL stands for a sustainable and secure energy future with innovative technology and the highest quality standards.

Continuous testing and training

Before each software release, the software of KOSTAL inverters undergoes extensive security testing. CVE scans are used to identify potential vulnerabilities, while external independent penetration tests provide additional security. Internally, KOSTAL relies on regular training: Every year, all employees take part in mandatory IT security training to ensure a high level of security in all areas.

Standards and certifications

While KOSTAL is currently working on compliance with the EU-wide “Cyber Resilience Act” (CRA), the inverters meet requirements such as RED, ETSI EN303645 and ISO 62443. With regard to the NIS2 directive, the responsibility for major projects for verification lies with the respective project operators.

Data protection and secure communication

Data protection is KOSTAL‘s top priority. All inverter monitoring data is stored on servers based on Azure technology in the EU – in data centers in the Netherlands and Germany. Personal data is not stored directly on the inverters. Communication with the devices is secured by encrypted and signed update files and personalized access control.

Maximum safety for users and installers

Unauthorized access is prevented by a multi-level security system. Changes to inverter parameters can only be made by authorized installers who have an individual password (service code) and a device-specific master key. In addition, all device communication ports (for control) are closed by default.

AutoUpdate for a secure future

All software updates are installed automatically in encrypted form using the KOSTAL AutoUpdate function. This guarantees that critical updates can be installed quickly and securely at any time. An integrated security function also blocks access after several failed login attempts.