

ANEC FACTSHEET: WILL THE NEW EUROPEAN STANDARDS ON CYBERSECURITY PROTECT CONSUMERS?

BACKGROUND

Connected products like wearables, home assistants, toys and appliances bring convenience and new services to consumers but they also expose them to new risks that traditional product safety and standards were not designed to address.

Since 2021, ANEC has supported the development of new mandatory requirements **on cybersecurity, privacy and fraud for consumers connected products** (Commission Delegated Regulation (EU) 2022/30 on essential requirements under Article 3(3)(d), (e) and (f) of the Radio Equipment Directive), adopted on **29 October 2021**. The new obligations should have started in August 2024 but were postponed to **August 2025** because of delays in the standardisation process.

This new law makes **data protection and security mandatory for connected products (radio equipment)**, addressing our longstanding concerns about insecure products, such as smart toys and smartwatches (e.g. Cayla “the spying doll”).



HARMONISED STANDARDS

To support the regulation, CEN-CENELEC developed three harmonised standards:

- **EN 18031-1:2024**: Internet connected radio equipment
- **EN 18031-2:2024**: Radio equipment processing data (including toys, childcare, wearables)
- **EN 18031-3:2024**: Radio equipment processing virtual money.



While contributing actively to the drafting process, ANEC was unable to support the approval of these standards due to concerns over vague requirements, unclear and non-reproducible testing methods, and potential challenges for effective market surveillance. These concerns were echoed by the HAS Consultant, who raised similar observations.



LATEST DEVELOPMENTS

On **28 January 2025**, the European Commission adopted **Implementing Decision (EU) 2025/138**, citing these three standards with restrictions in the Official Journal to provide presumption of conformity with the new rules as of **1 August 2025**.

The Commission also issued non-binding guidance to explain the restrictions, clarifying which parts of the standards **do not provide presumption of conformity and therefore lack legal certainty**.

ANEC'S POSITION

The restrictions are a positive acknowledgement of areas that need improvement and reflect many of the concerns ANEC has raised over time. However, we believe further work is needed to fully address the weaknesses we identified.

ANEC continues to highlight the need for stronger standards that:

- Include detailed, reproducible testing methodologies.
- Support market surveillance authorities in enforcing compliance effectively.
- Presumption of conformity is granted only where robust risk assessment provisions are in place.

We stress the need of strong market surveillance to guarantee enforceable consumer protection when the RED Delegated Act enters into application. We also look forward to the forthcoming standards under the **European Cyber Resilience Act**, which are expected to deliver a higher level of cybersecurity and protection for consumers.

Raising standards for consumers

The European consumer voice in standardisation aisbl

Rue d'Arlon 80, 1040 Etterbeek

Brussels, Belgium

[anec\(at\)anec.eu](mailto:anec(at)anec.eu)

+32 (0)2 743 24 70

www.anec.eu

X: [@anectweet](https://twitter.com/anectweet)

LinkedIn: [@anectweet](https://www.linkedin.com/company/anectweet)

Bluesky: [@raisingstandardseu.bsky.social](https://bsky.app/profile/raisingstandardseu.bsky.social)

ANEC is supported financially by the European Union & EFTA

