Radio Equipment Directive Delegated Act (EU) 2022/30			
Official Source	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0030		
Geographic Region	European Union	affected industries	cross-industry
Scope	Internet-connected radio equipment and wearable radio equipment		
In brief	1. radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service 2. radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected 3. radio equipment supports certain features ensuring protection from fraud		
Consequences	Non-compliance with the Directive may result in products being prohibited from sale in the EU market, enforcement actions by regulatory authorities, and potential financial and reputational damage to the manufacturer.		
Baseline Standard	EN 18031-1:2024 EN 18031-2:2024 EN 18031-3:2024		

The European Commission (EC) has advanced efforts to enhance cybersecurity for Internet-connected radio equipment within the EU by implementing a delegated act under the Radio Equipment Directive (RED). While initially set for enforcement in August 2024, the regulation's start date has been extended to 1st August 2025, to allow time for the development of harmonized standards. Beginning on this date, in-scope wireless devices and products sold in the EU must comply with the requirements set by the RED Delegated Act (EU) 2022/30. Throughout this document, the Radio Equipment Directive as modified by Delegated Regulation (EU) 2022/30 will be referenced as "RED DA"

To provide guidance on implementing cybersecurity measures for radio equipment, ensuring devices meet essential RED DA requirements for network security, data privacy, and fraud protection as defined in Articles 3(3)(d), (e), and (f) of the EU's Radio Equipment Directive, the EN 18031 standard was developed by the European Committee for Standardisation (CEN) and European Committee for Electrotechnical Standardisation (CENELEC) and adopted by the European Union on 30th January 2025.

The EN18031 standard is structured into three parts, each addressing different aspects of cybersecurity for Internet-connected radio equipment:

1. **EN18031-1:2024**: Covers general security requirements for radio equipment, addressing network security risks.
2. **EN18031-2:2024**: Focuses on data and privacy protections for devices handling personal or sensitive data, including IoT devices like wearables and toys.
3. **EN18031-3:2024**: Pertains to devices handling virtual or monetary values, focusing on fraud protection.

It is important to note that the three parts of EN 18031 are not necessarily mutually exclusive. Depending on the functionality and risk profile of a device, one or more parts may apply in parallel. It is therefore important to understand the risk profile of your device and determine which sections impact you.

The EN 18031 standard includes decision trees and pass/fail criteria to help manufacturers evaluate product compliance and mitigate vulnerabilities effectively. The standards are set to become mandatory from 1st August 2025, aligning with RED DA's deferred cybersecurity enforcement date.

1. Does RED DA apply to me?

The Radio Equipment Directive (RED) delegated act on cybersecurity ("RED DA") will apply to you if you manufacture, import, or sell internet-connectable radio equipment in the European Union.

Specifically, the delegated act applies to:

- Most radio equipment that is directly or indirectly connectable to the Internet, such as IoT devices, industrial machinery, consumer electronics, and other equipment with a radio interface. This encompasses any electrical or electronic product capable of Internet communication, either directly or through intermediary devices. This broad scope reflects the growing reality that even devices not traditionally seen as 'Internet-connected' - for example, those communicating via Bluetooth, Zigbee, or proprietary wireless protocols - could still form part of Internet-connected systems when paired with gateways, smartphones, or networked controllers. Therefore, such equipment falls under the same baseline cybersecurity expectations as devices with native Internet access using the Internet Protocol (IP) as transmission protocol. Despite differing interpretations, with some stakeholders arguing that only devices communicating via IP should be considered 'Internet-connected', the prevailing