Radio Equipment Directive (RED)

From 1st August 2024, all new and existing products placed on the EU market under the scope of the Radio Equipment Directive (RED) must comply with the new cyber security requirements. Ensure your products are compliant to place them on the EU-27 market today.

Thanks to the rapid expansion of products using technologies such as Wi-Fi, NFC, and Bluetooth, the risk of a cyber attack or identity/financial fraud, to both consumers and businesses, has grown significantly over recent years.

To help mitigate these risks, in October 2021 the European Commission adopted a delegated act to the RED (2014/53/EU) so that all wireless devices placed on the EU-27 market are safe and suitable for use.

Published in the Official Journal of the EU (OJEU) on the 12th January 2022, and mandatory from the 1st of August 2024, the changes increase the cyber security, personal data privacy, and fraud protection for applicable wireless devices available on the EU market and enforce compliance requirements to RED Articles:

- 3.3 (d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of services
- 3.3(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected
- 3.3(f) radio equipment supports certain features ensuring protection from fraud

What products will these changes impact?

The changes will impact manufacturers who are declaring to the RED.

Products that fall under the scope of these changes include:
- wireless devices such as mobile phones, tablets and other products capable of communicating over the internet
- toys and childcare equipment such as baby monitors
- wearable equipment such as smart watches or fitness trackers

What actions do manufacturers need to take?

Manufacturers should prepare for the August 2024 deadline by undertaking a review of both existing products and new product designs to assure that they will comply with the new cyber security requirements.

What standards do products need to be testing against to show conformity?

Currently, there are no harmonised standards. Therefore, manufacturers should consider testing to existing standards such as EN 303 645 using the requirements detailed in TS 103 701. These will likely be used as a basis for future harmonised standards, so testing and certifying products to these will ensure readiness prior to the August 2024 deadline.

In the absence of harmonised standards, products will need a conformance certification issued by an EU Notified Body. As an EU Notified Body for the (RED), Resillion and Eurofins E&E provide manufacturers with testing and certification against ETSI EN 303 645 and TS 103 701, allowing products to meet the requirements of the RED and providing manufacturers with a route to continued market access.