Ready, RED, Go?

Anforderungen der Radio Equipment Directive für Geräte mit Internetverbindung ab 1. August 2025

03 July 2025

Zum 1. August 2025 treten für eine Vielzahl von elektronischen Geräten weitere Cybersicherheitsanforderungen gemäß der Richtlinie über die Bereitstellung von Funkanlagen auf dem Markt (RL 2014/53/EU; Radio Equipment Directive oder RED) in Kraft. Trotz des nahenden Stichtages sind noch viele Themen unklar, insbesondere der Anwendungsbereich der neuen Regelungen und die Auslegung des Begriffs der „mit dem Internet verbundenen Funkanlagen".

Überblick über die RED

Die RED legt bestimmte Produktsicherheitsstandards für Funkanlagen fest. Als Funkanlagen zählen dabei jegliche Geräte, die Radiowellen zu Kommunikations- oder Ortungszwecken ausstrahlen oder empfangen können. Neben dem klassischen Radio fallen hierunter alle Geräte mit Internetverbindung oder Bluetooth-Anschluss, also Handys, Notebooks, WLAN-Router, GPS-Tracker etc. Die meisten dieser Produktanforderungen sind seit 13. Juni 2017 in Kraft, gelten also für alle Geräte, die nach diesem Tag in Verkehr gebracht wurden. In Deutschland dient das Funkanlagengesetz (FuAG) der Umsetzung der RED.

Nachträglich sind viele weitere Anforderungen dazugekommen, so auch für einheitliche Ladegeräte, die zum 28. Dezember 2024 in Kraft getreten sind.

Neue Anforderungen für mit dem Internet verbundene Funkanlagen

Für einige Vorschriften muss die Europäische Kommission bestimmte Produktkategorien festlegen, die von der Vorschrift erfasst werden sollen, so auch Art. 3 Abs. 3 RED. In Deutschland gilt diese Regelung unmittelbar kraft § 4 Abs. 3 FuAG. Art. 3 Abs. 3 Buchst. d-f RED erheben technische Anforderungen in Hinsicht auf Netzwerksicherheit, Datenschutz und Betrugsschutz, die im Einzelnen von europäischen Normungsorganisationen wie dem Europäische Komitee für Normung (CEN) konkretisiert werden.

Mit der delegierten VO 2022/30/EU hat die Kommission nunmehr Art. 3 Abs. 3 Buchst. d-f RED „aktiviert". Für die Netzwerksicherheitsanforderungen hat das CEN die harmonisierten Standards EN 18031-1, für den Datenschutz 18031-2 sowie für den Betrugsschutz EN-18031-3 erarbeitet. Die technischen Anforderungen der EN 18031-1 umfassen unter anderem Mechanismen zur Zugangskontrolle, zur Authentifizierung, zur sicheren Kommunikation sowie zur Netzwerküberwachung.

Anwendungsbereich von Art. 3 Abs. 3 Buchst. d-f RED

Anwendbar sind diese neuen Standards aber nicht für alle Funkanlagen im Sinne der RED. Vielmehr gelten sie nur für Funkanlagen, die selbst über das Internet kommunizieren können, unabhängig davon, ob sie direkt oder über andere Geräte kommunizieren („mit dem Internet verbundene Funkanlagen"). Unproblematisch sind damit alle Geräte gemeint, die direkt Daten über das Internet empfangen oder senden können, also Smartphones, Laptops, sowie diverse Smart Home-Geräte.

Zu beachten ist, dass die Internetverbindung nicht notwendigerweise über Radiowellen erfolgen muss. Es sind auch Geräte erfasst, die zwar bestimmte Daten per Radiowellen versenden oder empfangen können, aber nur per Kabel mit dem Internet verbunden sind. Darunter fallen vor allem WiFi-Router.

Schwieriger ist die Frage, inwieweit auch Geräte umfasst sind, die nicht direkt mit dem Internet verbunden sind, sondern nur über andere Geräte Daten an das Internet versenden und empfangen können. Das sind bspw. Geräte, die über Bluetooth Daten mit internetfähigen Geräten austauschen, so vor allem kabellose Kameras, Mikrofone, Sensoren, etc. Interessenverbände setzen sich dafür ein, dass als mit dem Internet verbundene Funkanlagen nur solche zählen, die auch selbst internetfähige Protokolle ausführen können. Damit wären Bluetooth-Geräte nicht erfasst. Die zuständigen Aufsichtsbehörden (u. a. in Deutschland die Bundesnetzagentur) lassen bisher keine klare Linie erkennen, ebenso wenig die Europäische Kommission, die mit ihrem RED Guide grundsätzlich Auslegungshilfen bietet.

Darüber hinaus gelten die Datenschutzanforderungen nach Art. 3 Abs. 3 Buchst. e RED auch für Funkanlagen, die der Kinderbetreuung dienen (sog. Babyphones), Spielzeug im Sinne der RL 2009/48/EG, sowie Funkanlagen, die am Körper getragen werden. Unter letzteres zählen vor allem Smartwatches.

Dagegen sind Medizinprodukte im Sinne von VO 2017/745/EU und In-Vitro-Diagnostika im Sinne von VO 2017/746/EU vom Anwendungsbereich der Art. 3 Abs. 3 Buchst. d-f RED ausgenommen.

Weitere EU-Cybersicherheitsvorgaben

In Sachen Cybersicherheit von Produkten sind nicht nur die Vorgaben der RED zu beachten. Überlappungen sind denkbar mit der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau (RL 2022/2555/EU; NIS-2-Richtlinie) oder der Verordnung über horizontale Sicherheitsanforderungen für Produkte mit digitalen Elementen (VO 2024/2847/EU; Cyber Resilience Act oder CRA).

Die NIS-2-Richtlinie stellt Sicherheitsanforderungen an die Betreiber von kritischen Infrastrukturen. Die Umsetzungsfrist für die Mitgliedstaaten ist zwar bereits am 18. Okto-

ber 2024 abgelaufen, jedoch haben bisher nur neun Mitgliedstaaten die Richtlinie umgesetzt, darunter Belgien und Italien. Während in den Niederlanden und Österreich eine Umsetzung noch dieses Jahr erwartet wird, ist in Frankreich, Spanien und Deutschland mit einer wesentlich späteren Umsetzung zu rechnen. So hat das deutsche Bundesinnenministerium erst Ende Mai 2025 einen Referentenentwurf zur Umsetzung der NIS-2-Richtlinie veröffentlicht, womit es noch bis nächstes Jahr dauern dürfte, bis das Gesetz in Kraft tritt.

Der CRA stellt bestimmte Anforderungen an Produkte mit digitalen Elementen mit Netzwerkverbindung. Die in Anhang I Teil I gelisteten Cybersicherheitsanforderungen umfassen Kontrollmechanismen gegen unautorisierten Zugang, Datenverschlüsselung sowie die Überwachung interner Aktivitäten. Der CRA tritt am 11. Dezember 2027 in Kraft. Als Verordnung gilt er unmittelbar und bedarf keiner Umsetzung durch die Mitgliedstaaten.

Im Gegensatz zur RED erfasst der CRA auch Geräte ohne Radiofunktion, also auch für Geräte, die Daten nur per Kabel versenden und empfangen. Die Cybersicherheitsanforderungen beider Rechtsakte überschneiden sich in erheblichem Maße. Generell ist davon auszugehen, dass die CRA-Anforderungen umfassender und strenger sind als die in Art. 3 Abs. 3 Buchst. d RED. Teilweise wird sogar angenommen, dass die CRA die RED-Cybersicherheitsanforderungen obsolet machen wird.

Fazit

Trotz klarer technischer Standards bestehen nach wie vor offene Fragen zum Anwendungsbereich der RED, insbesondere in Hinsicht auf Geräte mit indirekter Internetverbindung. Weitere Unsicherheiten bestehen bei der Abgrenzung zur NIS-2-Richtlinie und zum CRA. Für Hersteller ist deshalb eine frühzeitige, umfassende Auseinandersetzung mit den EU-Cybersicherheitsanforderungen zu empfehlen. Dazu ist die gewissenhafte Durchführung eines Konformitätsbewertungsverfahrens nach Art. 17 RED unabdinglich.

BLOMSTEIN wird die weiteren Entwicklungen verfolgen und darüber informieren. Zu allen Fragen in Sachen Produktregulierung und Cybersicherheit steht Ihnen Dr. Leonard von Rummel jederzeit zur Verfügung.

***