Cybersicherheit und Datenschutz bei Funkanlagen

Ein Beitrag von Stefan Hessel

EU-Kommission will Hersteller verpflichten!

Seit Jahren häufen sich IT-Sicherheitsvorfälle und Datenschutzverletzungen im Zusammenhang mit dem Internet of Things (IoT), vernetzten Spielzeugen und Wearables. Darauf reagiert die EU-Kommission jetzt mit einem Entwurf für eine delegierte Verordnung zur Radio Equipment Directive (RED), zu dem bis zum 27. August 2021 eine öffentliche Konsultation läuft. Mit der Verordnung will die Kommission den Art. 3 Abs. 3 lit. d)-f) RED mit Leben füllen und Hersteller zu Maßnahmen in Bezug auf Cybersicherheit, Datenschutz und Betrugsprävention verpflichten.

Als Teil der RED sind die Vorgaben im Rahmen des Konformitätsbewertungsverfahrens (Art. 17 RED) zu berücksichtigen und damit erforderlich für die CE-Kennzeichnung von Funkanlagen und die Bereitstellung der Geräte auf dem europäischen Markt. Hersteller entsprechender Geräte werden durch die Kommission damit unmittelbar zur Umsetzung von Cybersicherheit, Datenschutz und Betrugsprävention verpflichtet. Im Folgenden möchten wir Sie daher ausführlich zu diesem für Hersteller hochrelevanten Thema informieren.

Cybersicherheit, Datenschutz, Betrugsprävention – was bald für Hersteller gelten könnte

Verabschiedet die EU-Kommission die delegierte Verordnung in der aktuellen oder ähnlichen Form, müssen die Hersteller von Funkanlagen künftig zwingend Maßnahmen zur Cybersicherheit, zum Datenschutz und zur Betrugsprävention ergreifen, um ihre Geräte rechtskonform auf dem europäischen Markt bereitzustellen. Welche Maßnahmen genau erforderlich sind, hängt von der Art der Funkanlage ab:

- Funkanlagen, die mit dem Internet verbunden sind, sollen künftig die Anforderungen an die Cybersicherheit nach Art. 3 Abs. 3 lit. d) RED erfüllen. Die Geräte dürfen folglich weder schädliche Auswirkungen auf das Netz oder seinen Betrieb haben noch eine missbräuchliche Nutzung von Netzressourcen, die eine unannehmbare Beeinträchtigung des Dienstes verursachen, erlauben. Entsprechende Maßnahmen wären damit für alle IoT-Geräte verpflichtend.

- Anforderungen an den Datenschutz nach Art. 3 Abs. 3 lit. e) RED sollen künftig alle Funkanlagen erfüllen, mit denen personenbezogene Daten nach Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) oder Verkehrs- bzw. Standortdaten nach Art. 2 lit. b) und c) der ePrivacy-Richtlinie verarbeitet werden und die

1. mit dem Internet verbunden sind oder
2. ausschließlich zur Kinderbetreuung konzipiert und bestimmt sind (z.B. Babyphon) oder
3. Spielzeug im Sinne der Spielzeugsicherheitsrichtlinie sind (z.B. Smart Toys) oder
4. Wearables, die am menschlichen Körper getragen oder mit diesem verbunden werden (z.B. Smart Watches, Smart Clothing, Kopfhöher, Fitnesstracker, vernetzte Schuhe etc.).

Konkret erforderlich ist in diesen Fällen, dass das Gerät über Sicherheitsvorrichtungen verfügt, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden.

- Kann ein Nutzer über eine Funkanlage am Zahlungsverkehr teilnehmen oder virtuelle Währungen verwalten, muss das Gerät Funktionen zum Schutz vor Betrug unterstützen und dadurch die Betrugsprävention unterstützen.

Der weitere Fahrplan: Verpflichtung geplant ab 2024

Die Konsultation der EU-Kommission zum Entwurf für den delegierten Rechtsakt läuft noch bis zum 27. August 2021. Die Annahme des Entwurfs durch die EU-Kommission ist bereits für das vierte Quartal 2021 geplant. In Kraft treten wird der Entwurf, der eine Umsetzungsfrist von 30 Monaten vorsieht, 20 Tage nach der Veröffentlichung im Amtsblatt der Europäischen Union. Hersteller können sich also darauf einstellen, dass sie die neuen Vorgaben spätestens Mitte 2024 umgesetzt haben müssen, wenn sie ihre Produkte weiterhin auf dem europäischen Markt bereitstellen wollen.

Unsere Empfehlungen für Hersteller

Dass Hersteller gesetzliche Anforderungen an Cybersicherheit und Datenschutz beachten müssen, ist nicht ganz neu. Bereits im Jahr 2017 hatte Stefan Hessel, der heutige Co-Head unserer Digital Business Unit, beispielsweise ein Verbot der vernetzten Spielzeugpuppe "My friend Cayla" durch die Bundesnetzagentur initiiert, weil die Puppe für Abhörzwecke missbraucht werden konnte. Darüber hinaus ist bereits nach der geltenden Rechtslage eine Verpflichtung der Hersteller zur Berücksichtigung der DSGVO nicht völlig ausgeschlossen. Es ist jedoch auch festzuhalten, dass sich die gesetzlichen Vorgaben mit zunehmender

Geschwindigkeit verdichten und es zu deutlichen Verschärfungen kommt. Mit Blick auf die lange Vorlaufzeit, die eine Anpassung von Produkten und die Umstellung der Produktentwicklung in Anspruch nehmen können, sollten Hersteller sich daher schnellstmöglich auf die Umsetzung der neuen Vorgaben vorbereiten. Weitere aktuelle Entwicklungen, wie das freiwillige IT-Sicherheitskennzeichen oder die Updatepflicht nach der Digitale-Inhalte-Richtlinie sollten dabei ebenfalls berücksichtigt werden. Idealerweise setzen Hersteller die gesetzlichen Vorgaben mithilfe eines Compliance Managementsystems um, da so die größtmöglichen Synergieeffekte zwischen den einzelnen regulatorischen Vorgaben erzielt werden können.

[August 2021]

Unternehmenskontakt: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E melanie.schaumann@reuschlaw.de