



Nové požadavky na kybernetickou bezpečnost u rádiových zařízení **RED DA (EU) 2022/30**

Legislativa: Co se mění od 1. 8. 2025?

Od 1. srpna 2025 vstoupí v platnost nové povinnosti vyplývající z Nařízení Komise v přenesené pravomoci (EU) 2022/30 ze dne 29. října 2021, kterým se doplňuje směrnice 2014/53/EU Evropského parlamentu a Rady, pokud jde o požadavky na kybernetickou bezpečnost rádiových zařízení. Tyto povinnosti reagují na rychlý rozvoj internetu věcí (IoT) a rostoucí hrozby kybernetických útoků.

V České republice se tímto zabývá **Nařízení vlády č. 426/2016 Sb.**, o posuzování shody rádiových zařízení při jejich dodávání na trh (dále jako "nařízení vlády").

Hlavní změny

- Povinnost prokázat kybernetickou bezpečnost rádiových zařízení připojených přímo nebo nepřímo do internetu.
- Závazné pro všechna nová zařízení uváděná na trh po 1. srpnu 2025.
- Týká se také zařízení již uvedených na trhu, které projdou významnou změnou (např. změna firmware, rozšíření funkcí ovlivňující bezpečnostní chování apod.).

Co to znamená pro výrobce?

Každý výrobce bude nově muset:



Zajistit soulad s technickými požadavky

Zajistit, aby rádiové zařízení bylo navrženo a vyrobeno v souladu s technickými požadavky nařízení vlády (§ 3, odst. 3, písm. d), e), f).



Vypracovat technickou dokumentaci

Vypracovat technickou dokumentaci podle přílohy č. 5 nařízení vlády, která musí obsahovat všechny relevantní informace pro posouzení shody zařízení.



Provést příslušný postup posouzení shody



Vypracovat EU prohlášení

Vypracovat a uchovávat EU prohlášení o shodě.



Umístit označení CE



Uchovávat dokumentaci

Uchovávat technickou dokumentaci a EU prohlášení o shodě po dobu 10 let od uvedení zařízení na trh.



Zajistit soulad sériové výroby

Zajistit, aby sériová výroba zůstala v souladu s požadavky nařízení vlády, a to i při změnách v konstrukci zařízení nebo použitých normách.

Kterých výrobků se nové požadavky týkají?

Nové požadavky na kybernetickou bezpečnost se vztahují na široké spektrum rádiových zařízení, která využívají připojení k internetu. Další požadavky se uplatní v případech, kdy zařízení zpracovává osobní údaje anebo pracuje s peněžními hodnotami.

Konkrétní příklady pro lepší představu:

Rádiová zařízení připojená k internetu – zajištění integrity a ochrany sítě (čl. 3 odst. 3 písm. d) RED)

Zařízení připojující se k internetu musí být konstruována tak, aby neměla nepříznivý vliv na síť elektronických komunikací nebo její provoz a nezneužívala zdroje sítě elektronických komunikací. Připojení k internetu může být i příležitostné nebo nepřímé.



Nejběžnější příklady:

- Domácí Wi-Fi routery
- Firemní směrovače
- LTE/5G modemové brány
- Mesh Wi-Fi systémy
- Přístupové body (Access Points)
- Chytré televizory s Wi-Fi, Smart reproduktory (Google Home, Amazon Echo)
- Chytré pračky s dálkovým ovládáním
- Chytré lednice s internetovým připojením, Průmyslové IoT gatewaye
- Bezdrátové tiskárny připojené k síti
- IP bezpečnostní kamery
- Dálkové ovládané termostaty (např. Nest)
- Elektronické zámky připojené k internetu
- Chytré měřiče energií (smart meters)

Rádiová zařízení připojená k internetu – ochrana osobních údajů (čl. 3 odst. 3 písm. e) RED)

Zařízení zpracovávající osobní údaje, lokalizační informace, zdravotní data apod. Nad rámec zajištění integrity a ochrany sítě tak musí výrobce zajistit i ochranu osobních údajů.

Nejběžnější příklady:

- Chytré hodinky (Apple Watch, Samsung Galaxy Watch)
- Fitness náramky (Fitbit, Garmin)
- Chůvičky s kamerou (baby monitors)
- Wearable EKG senzory
- Glukometry s mobilní aplikací
- Monitorovací náramky pro seniory
- Interaktivní chytré hračky
- Domácí IP kamery s cloudovým uložením
- GPS sledovače domácích mazlíčků
- Chytré brýle s AR funkcemi
- Virtuální asistenti rozpoznávající hlas (Alexa, Google Assistant)
- Mobilní aplikace pro sledování spánku (napojené na senzory)
- Biometrické přístupové systémy (otisky prstů, rozpoznávání tváře)
- Mobilní zařízení se zdravotními aplikacemi
- Chytré váhy měřící BMI a složení těla

Rádiová zařízení připojená k internetu – ochrana proti podvodům (čl. 3 odst. 3 písm. f) RED)

Zařízení umožňující nebo provádějící elektronické platby, správu financí, kryptoměny. Nad rámec zajištění integrity a ochrany sítě tak musí výrobce zajistit i ochranu proti podvodům.

Nejběžnější příklady:

- Platební terminály (POS)
- Mobilní telefony podporující NFC platby
- Chytré hodinky s bezkontaktními platbami
- Hardware kryptopeněženky (Ledger, Trezor)
- Mobilní aplikace pro virtuální platby
- Bezkontaktní mytné jednotky ve vozidlech
- Parkovací automaty s bezkontaktní platbou
- Elektronické pokladní systémy (e-kasa)
- Platební brány v automatech na jízdenky
- Samoobslužné kiosky v restauracích (např. McDonald's)
- Platební zařízení v taxislužbách
- Přenosné pokladny pro trhy a festivaly
- Systémy mikroplateb v mobilních hrách
- Platební moduly v e-scooterech a sdílených kolech
- Automatizované systémy pro placení parkovného



Jak prokázat shodu s novými požadavky RED?

Každý výrobce, který uvádí na trh rádiové zařízení spadající pod směrnici RED (2014/53/EU) a Delegovaný akt (EU) 2022/30, musí prokázat, že jeho výrobek splňuje všechny legislativní požadavky, včetně těch nově zavedených v oblasti kybernetické bezpečnosti.

Tento proces se nazývá posouzení shody a je to nezbytný krok k tomu, aby výrobek:

- mohl být označen značkou CE,
- mohl být legálně uveden na trh EU,
- byl v souladu s platnou legislativou a nedošlo k riziku sankcí nebo jeho stažení z trhu.

Během posouzení shody se ověřuje, zda:

- Byly splněny nové požadavky na kybernetickou bezpečnost, pokud výrobek podléhá rozsahu čl. 3(3) směrnice RED.
- Technická dokumentace je úplná, aktuální a správně strukturovaná.
- Výrobek byl posouzen dle příslušných harmonizovaných norem (zejména EN 18031-1 až -3).
- Je doloženo, že sériová výroba bude v souladu s hodnoceným typem nebo systémem kvality.

Cesty k posouzení shody:

Modul A

Interní kontrola výroby
(Self-Declaration)

Modul B

EU Přezkoušení typu
(Type Examination)

Modul H

Zajištění kvality výroby
(Full Quality Assurance)

Jak probíhá posouzení shody ze strany oznámeného subjektu?

1. Volba modulu

Výrobce zvolí vhodný modul posouzení shody (B nebo H – viz výše).

2. Příprava dokumentace

Výrobce připraví nebo doplní požadovanou technickou dokumentaci.

3. Posouzení

Posouzení notifikovanou osobou – dle zvoleného modulu.

4. Vydání certifikátu

Po úspěšném dokončení posouzení je vydán certifikát EU přezkoušení typu nebo zpráva z auditu, na jejichž základě výrobce může vystavit EU prohlášení o shodě a výrobek může být označen značkou CE a legálně uveden na trh EU.

Modul A – Interní kontrola výroby (Self-Declaration)

Co to znamená?

1. Výrobce sám provede posouzení shody svého zařízení.
2. Na základě výsledků testování vypracuje a podepíše EU prohlášení o shodě.
3. Není nutné zapojení oznámeného subjektu (žádné externí schválení).

Modul B EU Přezkoušení typu (Type Examination)

Co to znamená?

1. Výrobce předloží technickou dokumentaci k posouzení oznámenému subjektu.
2. Oznámený subjekt provede přezkum technické dokumentace a ověří, zda splňuje požadavky příslušné legislativy.
3. Výsledkem je vydání Certifikátu EU přezkoušení typu, který potvrzuje shodu typu výrobku.

Modul B je určen pro:

- Výrobky vyráběné v jednotlivých sériích nebo stabilních verzích.
- Výrobky, kde není potřeba zvláštní certifikace celého výrobního procesu.
- Výrobce, kteří chtějí certifikovat jednotlivé typy nebo modely zařízení.

Specifika Modulu B:

- Posuzuje se konkrétní typ výrobku.
- Certifikát se vztahuje pouze na certifikovaný typ – každá zásadní změna výrobku vyžaduje nové posouzení nebo aktualizaci certifikátu EU Přezkoušení typu
- Modul B nezahrnuje dohled nad výrobním procesem.

Modul H Zajištění kvality výroby (Full Quality Assurance)

Co to znamená?

1. Výrobce zavede a provozuje systém řízení kvality, který zajistí, že všechny vyráběné produkty budou trvale v souladu s požadavky směrnice RED a Delegovaného aktu (EU) 2022/30.
2. Notifikovaná osoba provádí posouzení systému kvality a jeho fungování v praxi.
3. Výsledkem je Zpráva z auditu, která schvaluje systém kvality výroby.

Modul H je vhodný pro:

- Výrobce s velkosériovou výrobou nebo častými variantami produktů.
- Výrobce, kteří chtějí mít možnost sami vydávat EU prohlášení o shodě bez nutnosti znovu certifikovat každý jednotlivý typ.
- Firmy s robustním systémem kvality (např. podle ISO 9001), který lze rozšířit o požadavky kybernetické bezpečnosti.

Specifika Modulu H:

- Posuzuje se celý proces vývoje, výroby, kontroly kvality a zajištění shody.
- Výrobce je následně oprávněn deklarovat shodu všech vyrobených produktů bez nutnosti opakovaného posouzení jednotlivých typů.
- Notifikovaná osoba provádí pravidelný dohled a audity, aby ověřila, že systém kvality je stále funkční a odpovídá požadavkům.

Jaké služby vám můžeme nabídnout?

EZÚ poskytuje ucelený systém služeb pro výrobce, kteří budou povinni prokázat shodu svých výrobků s požadavky RED v oblasti kybernetické bezpečnosti:

1. Pre-check	2. Certifikace zařízení dle normy EN 18031	3. Posouzení shody Modul B EU přezkoušení typu	4. Posouzení shody Modul H zajištění kvality výroby
--------------	--	---	---

1. Pre-check

Pre-check je informativní a školicí služba, jejímž cílem je:

- seznámit výrobce s požadavky směrnice RED a Delegovaného aktu (EU) 2022/30,
- objasnit legislativní a technické rámce související s kybernetickou bezpečností rádiových zařízení,
- vysvětlit požadavky na technickou dokumentaci a její strukturu,
- informovat o metodice tvorby rozhodovacích stromů dle EN 18031

Pre-check slouží k tomu, aby účastníci lépe porozuměli povinnostem, které musí následně doložit v rámci posouzení shody, a umožňuje jim lépe připravit podklady nezbytné k zahájení certifikačního procesu nebo posouzení shody ze strany oznámeného subjektu.

Co Pre-check zahrnuje:

1. Úvod do problematiky RED a legislativní rámec

- Vysvětlení směrnice RED 2014/53/EU a Delegovaného aktu (EU) 2022/30.
- Přehled norem harmonizovaných s RED (EN 18031)
- Vztah RED k dalším evropským právním předpisům (např. Cyber Resilience Act).
- Informování o obecné struktuře certifikačního procesu a procesu posouzení shody.

2. Informace k technické dokumentaci

- Seznámení s obecnou strukturou a požadovanými náležitostmi technické dokumentace.
- Diskuse nad požadavky na správnou strukturu dokumentace dle EN 18031.

3. Informace k tvorbě rozhodovacích stromů

- Představení významu rozhodovacích stromů v procesu posouzení.
- Obecná metodika sestavení rozhodovacích stromů dle EN 18031.
- Diskuse o způsobech zavedení bezpečnostních mechanismu a jejich popisu v dokumentaci.

Po absolvování služby Pre-check by měl mít výrobce ucelený přehled o požadavcích a být schopen připravit potřebnou dokumentaci k podání Žádosti o certifikaci, popřípadě Žádosti o posouzení shody.

Upozornění: V rámci služby Pre-check neprovádíme konzultace, neposkytujeme doporučení a nerealizujeme přímé úpravy dokumentace. Služba je čistě informativní, aby byla zachována nestrannost, objektivita a nezávislost certifikačního orgánu a oznámeného subjektu.

2. Certifikace zařízení dle normy EN 18031

Důležitým krokem k prokázání souladu s novými požadavky směrnice RED na kybernetickou bezpečnost je absolvování posouzení podle harmonizovaných norem EN 18031.

Co zahrnuje certifikace dle EN 18031?

EN 18031 je rozdělena do tří částí, přičemž:

- **Část 1 (EN 18031-1)** je povinná pro všechna rádiová zařízení spadající pod požadavky kybernetické bezpečnosti RED.
- **Část 2 (EN 18031-2)** a **část 3 (EN 18031-3)** jsou povinné, v závislosti na funkcionalitě, účelu a rizikovém profilu konkrétního zařízení.

Výrobce si podle charakteru svého zařízení určuje, zda je vhodné zařízení posoudit i dle částí 2 a 3.

Po úspěšném dokončení posouzení obdrží výrobce:

- Test Report (Zkušební protokol) - Oficiální dokument shrnující průběh a výsledky všech provedených posouzení podle EN 18031.
- Certifikát – Dokument potvrzující, že výrobek úspěšně absolvoval posouzení dle požadavků norem EN 18031.



3. Posouzení shody Modul B – EU přezkoušení typu

Modul B je určen pro výrobce, kteří chtějí nechat posoudit konkrétní typ výrobku – tedy jeho návrh, technickou dokumentaci a případné zkoušky. EZÚ jako notifikovaná osoba ověřuje, že navržené řešení splňuje všechny požadavky na kybernetickou bezpečnost a další technické náležitosti dle směrnice RED a Nařízení vlády č. 426/2016 Sb.

Jak to probíhá?

1. Zákazník podá žádost o EU přezkoušení typu, která zahrnuje technickou dokumentaci a podpůrné důkazy.
 2. EZÚ žádost zkontroluje, určí časovou náročnost na základě, které připraví cenovou nabídku a uzavře se zákazníkem smlouvu.
 3. Odborný tým EZÚ provede přezkum dokumentace – ověřuje správnost návrhu, rozsah a obsah zkoušek a případně požádá o doplnění.
 4. Je-li vše v pořádku, vypracuje se Hodnotící zpráva.
 5. Na základě výsledku je vydán Certifikát EU přezkoušení typu, který umožňuje uvést konkrétní výrobek na trh EU.
 6. Zákazník je povinen hlásit případné změny ve výrobku či technologiích. EZÚ na základě toho určuje, zda je nutné provést další přezkum a aktualizaci Certifikátu EU přezkoušení typu.
-

4. Posouzení shody Modul H – Zajištění kvality výroby

Modul H je postup posouzení shody, ve kterém se ověřuje, že výrobce má zavedený a funkční systém řízení kvality, díky kterému může trvale vyrábět zařízení ve shodě s požadavky. Nejedná se o posouzení jednoho výrobku, ale celého systému výroby.

Jak to probíhá?

1. Zákazník podá žádost o posouzení systému kvality, přiloží technickou dokumentaci a popis systému.
2. EZÚ žádost vyhodnotí a určí časovou náročnost služby, na základě které připraví cenovou nabídku a uzavře se zákazníkem smlouvu.
3. Odborný auditorský tým provede posouzení dokumentace systému kvality – sleduje, jak výrobce definuje odpovědnosti, kontrolní mechanismy, dokumentaci procesů a záznamy.
4. Následuje audit přímo u výrobce – posuzují se praktické aspekty fungování systému kvality a jeho napojení na konkrétní produkty.
5. Výsledky se shrnou v Zprávě z auditu, která slouží jako podklad pro rozhodnutí o vydání schválení systému kvality.
6. EZÚ provádí pravidelné roční dohledy a audity, aby ověřil, že systém zůstává funkční. Přičemž může ze strany EZÚ dojít i k neohlášeným kontrolám.

ezù m