Informace pro uživatele dle nařízení Data Act (EU 2023/2854)

Produktová řada: Routery Turris
Vydavatel: CZ.NIC, z.s.p.o., se sídlem Milešovská 1136/5, 130 00 Praha 3, IČO: 67985726, DIČ: CZ67985726
Zapsáno v spolkovém rejstříku vedeném u Městského soudu v Praze, sp. zn. L 58624

Verze dokumentu: 1.0
Datum účinnosti: 4. 9. 2026

Router Turris může během svého používání generovat data ve smyslu nařízení Data Act. Rozsah, formát, objem a povaha generovaných dat závisí na tom, které funkce uživatel aktivuje. Níže uvádíme povinné informace o tom, jaká data mohou vznikat, jak jsou zpracovávána, kde jsou ukládána, jak jsou přenášena a jaká práva má uživatel.

1. Generování dat v továrním nastavení

Router Turris je v základním (továrním) nastavení nakonfigurován jako pasivní síťová infrastruktura. V tomto režimu zařízení negeneruje ani neodesílá data, která by naplňovala definici „dat generovaných používáním zařízení“ podle čl. 2 odst. 1 Data Act. Základní síťový provoz (směrování paketů, připojení k internetu) nevede k vytváření dat, která by byla přenášena mimo zařízení nebo ukládána způsobem relevantním pro nařízení Data Act.

2. Volitelné funkce, které mohou generovat data

Generování dat ve smyslu nařízení Data Act nastává pouze při dobrovolné aktivaci níže uvedených softwarových subsystémů. Tyto subsystémy jsou v továrním nastavení vypnuté.

2.1 Turris Sentinel (bezpečnostní telemetrie)

- **Typ dat:** metadata o zachycených síťových útocích (např. IP adresy útočníků, typ útoku, časová razítka).
- **Předpokládaný objem dat:** cca tisíc eventů denně, v závislosti na intenzitě útoků.
- **Formát dat:** JSON / Msgpack; ukládání v PostgreSQL.
- **Ukládání:** data se neukládají lokálně; jsou odesílána nepřetržitě v reálném čase na servery CZ.NIC, kde jsou uchovávána po dobu jednoho roku.
- **Přenos:** zabezpečený kanál (MQTT/TLS).
- **Účel:** analýza kybernetických hrozeb a zajištění bezpečnosti.
- **Přístup uživatele:** prostřednictvím průběžně aktualizovaného dashboardu Sentinel (může obsahovat krátké zpoždění).
- **Sdílení s třetí stranou:** agregovaná statistická data (v rozsahu dat na dashboardu) je možné sdílet na žádost uživatele pouze pro účely zajištění bezpečnosti; surové IP adresy útočníků představují osobní údaje, jejich předání třetí straně je přípustné výhradně pro účely zajištění síťové a informační bezpečnosti (oprávněný zájem uživatele/příjemce dle GDPR); třetí strana nesmí tato data použít k žádnému jinému účelu a sdílení může vyžadovat technické záruky nebo NDA k ochraně integrity sítě.

2.2 Pakon / Morče (monitoring domácí sítě)

- **Typ dat:** statistiky síťových toků (NetFlow/IPFIX), přehled navštívených domén, IDS alerty.
- **Předpokládaný objem dat:** 1 záznam v databázi pro každé aktivní spojení
- **Formát dat:** IPFIX/NetFlow, SQLite databáze.
- **Ukládání:** výhradně lokálně na routeru (adresáře `/srv/morce`, `/srv/pakon`).
- **Retence:** automatická rotace dat při zaplnění vyhrazené kapacity; starší záznamy se přepisují.
- **Přenos:** žádný přenos mimo zařízení.
- **Přístup uživatele:** nepřetržitý a v reálném čase přes lokální rozhraní reForis nebo SSH (přímý přístup do SQLite databáze).
- **Sdílení s třetí stranou:** možné na žádost uživatele; protože jde o osobní údaje, sdílení vyžaduje právní titul dle GDPR.

2.3 Updater / Seznam balíčků

- **Typ dat:** informace o aktuální verzi softwaru, revizi hardwaru a seznamu nainstalovaných balíčků.
- **Předpokládaný objem dat:** 10 MiB denně
- **Formát dat:** textové dotazy přes HTTPS.
- **Ukládání a retence:** lokálně na zařízení; na serverech sdružení CZ.NIC se neukládají trvalé uživatelské profily.
    - Statistiky (používané verze TOS, IP protokoly, země...): zpracovává se prakticky v reálném čase; logy jsou potřeba jen do doby, než si je zpracuje ELK stack pro statistiky (řádově max. hodiny).
    - Monitoring: logy jsou potřeba pouze do doby zpracování nástrojem Zabbix (řádově max. hodiny).
    - Diagnostika: vzhledem k řešení problémů s uživateli i s časovým odstupem jsou logy uchovávány za posledních ukončených 6 měsíců.
    - Zálohy logů: uchovávají se po dobu 120 dnů (obecná výchozí doba retence záloh). Zálohy jsou uloženy na samostatném serveru a jsou zašifrovány.
- **Přenos:** šifrované dotazy přes HTTPS.
- **Přístup uživatele:** nepřetržitý přístup přes reForis nebo SSH.
- **Sdílení s třetí stranou na žádost uživatele: ANO** – data neobsahují osobní údaje ani obchodní tajemství, jejich předání nepodléhá omezením.

3. Práva uživatele podle Data Act

Uživatel má tato práva:

- **Právo na přístup k datům** generovaným aktivovanými funkcemi, a to v reálném čase u lokálně ukládaných dat (Pakon/Morče) nebo prostřednictvím průběžně aktualizovaných přehledů u cloudových služeb (Sentinel).

- **Právo na přenositelnost dat**, včetně možnosti poskytnout data třetí straně.
- **Právo na bezplatný a nepřetržitý přístup** k datům prostřednictvím lokálního rozhraní (reForis, SSH).
- **Právo deaktivovat** kterékoliv volitelné funkce a tím okamžitě zastavit generování i přenos dat.

Uživatel může svá práva na přístup k datům a jejich přenositelnost uplatnit elektronicky prostřednictvím e-mailu: info@turris.cz.

4. Přístup třetích stran

Pokud uživatel poskytne data třetí straně, sdružení CZ.NIC umožní takový přístup za spravedlivých, přiměřených a nediskriminačních podmínek, jak stanoví čl. 8–12 nařízení Data Act.

5. Práva k datům, ochrana duševního vlastnictví a kybernetická bezpečnost

5.1 Rozsah přístupu uživatele k datům
Uživatel má v souladu s nařízením Data Act právo na přístup výhradně k datům, která jsou přímým produktem provozu jím užívaného hardwaru (dále jen „Provozní data“). Mezi Provozní data, k nimž má uživatel zajištěn přístup, patří:

- Surová telemetrická data generovaná zařízením
- Logy síťového provozu daného uzlu
- Objemy přenesených a zpracovaných dat
- IP adresy kybernetických útoků zachycené výhradně na konkrétním zařízení uživatele

5.2 Vyloučení přístupu a ochrana duševního vlastnictví
Právo na přístup se nevztahuje na data, která jsou výsledkem softwarové nadstavby, pokročilé komplexní analýzy a interní vývojové činnosti sdružení CZ.NIC (dále jen „Obohacená data a know-how“). Tato data jsou chráněna jako obchodní tajemství a autorské právo pořizovatele databáze podle příslušných právních předpisů. Výhradním vlastnictvím poskytovatele zůstávají:

- Struktura telemetrických metadat a interní klasifikační klíče útoků, které vykazují znaky tvůrčí činnosti a tvoří chráněnou strukturu databáze.
- Metody míchání a agregace dat pocházejících od různých uživatelů.
- Algoritmy a logika generování dynamického firewallu.

Upozornění: Podmínky užívání softwaru, ochrana autorských práv k firmwaru a případná omezení dekompilace či zpětného inženýrství zdrojových kódů se řídí Licenčním ujednáním s koncovým uživatelem (EULA) operačního systému Turris OS a obecně závaznými právními předpisy. Tento informační text slouží výhradně ke splnění předsmluvní informační povinnosti a tato licenční ujednání nemění.

5.3 Omezení a odmítnutí přístupu z důvodu kybernetické bezpečnosti
Sdružení CZ.NIC postupuje v souladu s nařízením Data Act (zejména čl. 4 odst. 2 a čl. 5 odst. 8) a předpisy o kybernetické bezpečnosti (např. NIS 2). Přístup k datům nebo jejich export třetím stranám může být v nezbytném rozsahu omezen, pozastaven nebo odmítnut výhradně na základě objektivních rizik, pokud by takové sdílení prokazatelně mohlo:

- Ohrozit bezpečnostní požadavky na samotný produkt (hardware a jeho ochranné funkce).
- Způsobit zranitelnost systému, kterou by útočníci mohli využít k obcházení firewallu.
- Ohrozit kybernetickou bezpečnost kritické informační infrastruktury, významných informačních systémů nebo provozovatelů základních služeb.

Jakékoli takové odmítnutí nebo omezení přístupu bude poskytovatelem řádně odůvodněno na základě konkrétních bezpečnostních rizik.

6. Právo na stížnost

Uživatel má právo podat stížnost u příslušného vnitrostátního dozorového orgánu v České republice (Český telekomunikační úřad a Úřad pro ochranu osobních údajů pro oblast ochrany osobních údajů), pokud se domnívá, že jeho práva podle nařízení Data Act byla porušena.