

PROHLÁŠENÍ K NAŘÍZENÍ CYBER RESILIENCE ACT (CRA)



DECLARATION REGARDING THE CYBER RESILIENCE ACT (CRA)

Vážení zákazníci,

v souvislosti s rostoucím důrazem na kybernetickou bezpečnost a v návaznosti na přijetí nového evropského nařízení Cyber Resilience Act – CRA (Regulation (EU) 2024/1781) si vám dovoluujeme představit náš přístup k zajištění bezpečnosti při výrobě plošných spojů (PCB).

Ačkoliv se nařízení CRA na naši činnost nevztahuje přímo, jakožto na výrobce pasivních komponent bez vlastního digitálního prvku, uvědomujeme si, že vámi vyvíjené produkty často obsahují digitální funkce.

Naším cílem je proto zajistit, abyste se na naše výrobky mohli spolehnout i z hlediska kybernetické bezpečnosti produktu v souladu s aktuální legislativou.

1. Naše opatření v oblasti kybernetické bezpečnosti

- Přestože CRA přímo nevyžaduje, aby výrobci PCB byli certifikováni v oblasti kybernetické bezpečnosti, naše společnost se řídí mezinárodně uznávanými bezpečnostními standardy, běžně používanými v elektronickém průmyslu.
- Dodržujeme principy směrnice NIS 2 (EU) 2022/2555, zejména v oblasti řízení rizik a ochrany informačních systémů.
- Pravidelně provádíme aktualizace IT systémů, máme zavedené řízení přístupů, zálohování dat, ochranu proti malwaru, používáme šifrování a zabezpečené přenosy dat.
- Informace od zákazníků (technická dokumentace, výkresy, prototypy) chráníme s maximální péčí a přenášíme je pouze zabezpečenými kanály a ctíme dohody o mlčenlivosti.

2. Návrh a výroba desek z pohledu bezpečnosti

- Naše výroba probíhá vždy na základě vámi schválené dokumentace.
- Vzhledem k tomu, že obvykle neznáme konkrétní aplikaci výsledného produktu, nemůžeme sami navrhovat bezpečnostní funkce desek z pohledu digitální bezpečnosti.
- I přesto bereme v potaz rizika, která by mohla mít dopad na integritu, dostupnost nebo důvěrnost finálního produktu.

3. Podpora během životního cyklu produktů

- Ačkoliv naše desky samy o sobě neobsahují software, chápeme potřebu dlouhodobého zajištění bezpečnosti.
- Poskytujeme vám potřebnou dokumentaci a specifikace, které mohou pomoci při bezpečnostních auditech a zajištění shody s CRA.
- V případě potřeby spolupracujeme při řešení požadavků na úpravy, revize nebo kompatibilitu komponent během životního cyklu produktu.

4. Součinnost při auditech a shodě s CRA

- Jsme připraveni poskytnout součinnost při vašich bezpečnostních auditech nebo posouzení shody s CRA či dalšími relevantními předpisy.

Dear Customers,

In response to the growing emphasis on cybersecurity and the adoption of the new European regulation Cyber Resilience Act – CRA (Regulation (EU) 2024/1781), we would like to share with you our approach to ensuring security in the manufacturing of printed circuit boards (PCBs).

Although the CRA does not directly apply to our company as a manufacturer of passive electronic components without embedded digital functionality, we understand that your final products often include digital features.

Therefore, our goal is to ensure that our components meet high security standards and align with current expectations in cyber resilience.

1. Our Cybersecurity Measures

- While the CRA does not require PCB manufacturers to be certified in cybersecurity, we follow internationally recognized security standards widely accepted in the electronics industry.
- We adhere to the principles of Directive NIS 2 (EU) 2022/2555, particularly regarding risk management and protection of information systems.
- Our practices include regular IT system updates, access control, data backup, malware protection, and secure data encryption and transfer.
- We handle customer information (e.g., technical documentation, drawings, prototypes) with the utmost care and ensure it is transmitted through secure communication channels and we respect principles of confidentiality.

2. Secure Product Design

- Our production is always based on designs approved by our customers.
- In most cases, we are not aware of the final application in which the PCB will be used; therefore, we cannot influence the digital security design of the end product.
- However, we do consider potential risks that may affect the integrity, availability, or confidentiality of the final application.

3. Lifecycle Security Support

- While our PCBs do not contain software, we fully understand the importance of long-term security.
- We provide technical specifications and documentation that support your security audits and compliance processes.
- If needed, we assist in managing updates, revisions, or compatibility issues throughout the product lifecycle to minimize potential security risks.

4. Support for CRA Compliance and Audits

- We are ready to cooperate with your security audits and compliance assessments required by CRA or similar regulatory frameworks.

PROHLÁŠENÍ K NAŘÍZENÍ CYBER RESILIENCE ACT (CRA)



DECLARATION REGARDING THE CYBER RESILIENCE ACT (CRA)

- Nabízíme podkladovou dokumentaci, záznamy o kvalitě, zkouškách a procesech, které vám mohou pomoci při prokazování shody.
- U aplikací s vyššími nároky na bezpečnost poskytujeme technickou konzultaci, abychom zajistili hladkou integraci našich PCB do vašich zařízení.

5. Dlouhodobé partnerství a odpovědnost

- Naším cílem je být pro vás stabilním a spolehlivým partnerem, který poskytuje produkty odpovídající moderním nárokům na bezpečnost a kvalitu.
- Usilujeme o to, aby naše výrobky měly dlouhou životnost, byly odolné vůči zranitelnostem a přispívaly ke stabilitě a bezpečnosti vašich koncových řešení.

I když se nařízení CRA (EU) 2024/1781 na naši výrobu nevztahuje přímo, děláme maximum pro to, abyste mohli naše produkty bez obav využívat i v aplikacích s vysokými nároky na bezpečnost.

Rádi vám v této oblasti poskytneme maximální podporu a potřebnou dokumentaci.

- We can provide quality and safety documentation, test records, and production process details to support your due diligence or third-party evaluations.
- For critical systems with higher cybersecurity requirements, we offer technical consultations to ensure smooth and secure integration of our PCBs into your end products.

5. Long-Term Partnership and Responsibility

- Our goal is to be a reliable, long-term partner delivering safe and high-quality components that support your secure production processes.
- We ensure our products have optimal durability and resilience, contributing to the overall security and reliability of your final devices.

Although Regulation (EU) 2024/1781 – Cyber Resilience Act (CRA) does not apply directly to PCB manufacturing, we are fully committed to providing everything needed to help ensure the security and compliance of your products.

V Boskovicích dne 20¹¹/₀₄ 25

Gatema

P2

Gatema PCB a.s. IČ: 269 22 299
Průmyslová 2503/2 DIČ: CZ08976295
CZ 680 01 Boskovice www.gatema.cz

Zdeněk Čápal
Ředitel / CEO

Gatema PCB