Stockholm, 7 April, 2025

Swedish Riksdag
SE 100 12 Stockholm

Dear Members of the Swedish Riksdag,

RE: Request by Small Business Technology Developer Community for the Protection of End-to-End Encryption to Support Sweden's Security and Economic Goals

ACT | The App Association is a trade association representing small businesses technology companies from across the European Union (EU). Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. **The App Association writes to strongly encourage the Riksdag to oppose the potential legislation, referred to as 'Ju2024/02286 Datalagring och åtkomst till elektronisk information'[1] that could weaken encryption under the pretext of combating serious crime.**

The legislation would force companies to store and provide law enforcement with access to their users' communications, including those that are end-to-end encrypted.[2] Complying with this requirement for end-to-end encrypted communications services will be impossible without forcing providers to create an encryption backdoor. While we recognise the importance of combating illicit activities, we strongly urge caution against any measures that would undermine the security and integrity of encryption, as such actions pose significant risks to privacy, cybersecurity, and economic competitiveness. This would create an unprecedented breach in end-to-end encryption technology, exploitable by both States and malicious actors. Such a measure is extremely dangerous. As many institutions, including the Swedish Armed Forces[3] and the European Data Protection Committee,[4] have repeated, this would weaken the level of protection of all communications and threaten the confidentiality of all exchanges.

---

[1] https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2024/11/utkast-till-lagradsremiss-datalagring-och-tillgang-till-elektronisk-information/

[2] https://isoc.se/wp-content/uploads/2025/01/Ju2024_02286-DFRI-ISOC-SE-SNUS.pdf

[3] Stated that [access requirements in End-to-end encrypted communication] "cannot be fulfilled without introducing vulnerabilities and backdoors that third parties can exploit". https://regeringen.se/contentassets/e22f777eb1964c258c5d9a21adb6a355/forsvarsmakten.pdf

[4] 'The new rules should also clearly allow users to use end-to-end encryption (without 'backdoors') to protect their electronic communications. Decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited.' Opinion 5/2016 of the European Data Protection Supervisor

The App Association's small business members both in and outside of Sweden know that in order to compete across consumer and enterprise markets, they must be able to reliably restrict data access to authorised users, ensure data remains accurate and unmodified, and guarantee information is available when needed by authorised users. End-to-end encryption is a primary tool for providing the trust and security of their customers. Attempts by governments, most recently Sweden, to mandate backdoors to encryption algorithms significantly undermines these goals.

The App Association fully supports efforts to combat organised crime, however, the currently debated legislation will not help accomplish this goal. Its implementation would deeply damage security and trust across the digital economy by creating flaws in algorithms that can be used to compromise data confidentiality, integrity, and access requisites.

It is impossible to reserve security backdoors for just the 'good guys'. If a door exists then bad actors can, and will, exploit it. Sweden's demand would set a precedent for other countries and regimes to demand similar access to encrypted private data, further reducing citizens' privacy and safety.

The damage that would be caused by the implementation of this new law to Swedish and European small businesses innovating and competing across the global digital economy is not hypothetical. As a prime example, government mandates in the 1990s for broadband internet providers to enable law enforcement agencies access to encrypted communications on their networks has directly led recently to the China-backed hacker group Salt Typhoon gaining unprecedented unauthorized access to swaths of sensitive data. While the magnitude of this breach of U.S. telecommunications carrier networks continues to be investigated, at this time it appears that Salt Typhoon's access was essentially unlimited. This ongoing episode is evidence that mandating unfettered access via backdoors to encrypted devices or data in transit will result in that access being exploited by unintended actors. The Salt Typhoon experience demonstrates that weakening encryption will expose businesses to more frequent breaches, creating an even greater risk for those already marginalised.

With cyber attacks to critical infrastructure increasing in both frequency and severity, the need for security that end-to-end encryption provides has never been more essential. A mandated weakening of encryption would undermine the acknowledgement made by the Swedish Armed Forces in January 2025, when they stated that, 'the country is subject to regular cyberattacks'.[5]

By mandating platforms to covertly compromise their security, the Riksdag would raise serious concerns about the security of products operating in Sweden, leading to investors and consumers questioning whether their products contain hidden security vulnerabilities mandated by the Riksdag and our members being unable to grow and create jobs in Sweden.

[5] https://www.forsvarsmakten.se/sv/aktuellt/2025/01/hybridoperationer-skadar-sverige/

The precedent the Riksdag would create may also force some of our members to consider withdrawing from the Swedish market to avoid the reputational risks associated with undermining their own product's security. Lastly, adopting such legislation would not only damage Sweden's standing in global security and innovation policy[6] but would also signal a retreat from its leadership role in these areas.

Sweden has the power to protect encryption standards, ensuring they remain strong enough to safeguard digital infrastructure without creating loopholes that compromise security. Accordingly, we request that the Riksdag vote against the proposed law and engage in a revised policy development process to ensure that end-to-end encryption supports Swedish national and economic security. Our community fully commits to participating in such a process, and to more broadly support policies that enhance security and innovation as well as the Sweden's global leadership.

Sincerely,

Mike Sax
Founder and Chairperson

Brian Scarpelli
Senior Global Policy Advisor

Maria Goikoetxea Gomez de Segura
Policy Manager

[6] Notably, the European Court of Human Rights (ECtHR) has condemned governments requiring companies to disclose encryption keys as disproportionate measures that breach human rights law. https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}.