

Stockholm, 3 september

Sveriges riksdag
SE 100 12 Stockholm

Kära ledamöter av Sveriges riksdag,

RE: Begäran från småföretagsutvecklingsgemenskapen om skydd av end-to-end-kryptering för att stödja Sveriges säkerhets- och ekonomiska mål

ACT | App Association är en branschorganisation som representerar små teknikföretag från hela Europeiska unionen (EU). Våra medlemmar är entreprenörer, innovatörer och oberoende utvecklare inom det globala app-ekosystemet som samarbetar med vertikala marknader inom alla branscher. Vi arbetar med och för våra medlemmar för att främja en politisk miljö som belönar och inspirerar innovation, samtidigt som vi tillhandahåller resurser som hjälper dem att skaffa kapital, skapa arbetstillfällen och fortsätta att utveckla fantastisk teknik. **App Association skriver för att starkt uppmana riksdagen att motsätta sig den potentiella lagstiftningen, kallad "Ju2024/02286 Datalagring och åtkomst till elektronisk information"¹, som skulle kunna försvaga krypteringen under förevändning av att bekämpa grov brottslighet.**

Lagstiftningen skulle tvinga företag att lagra och ge brottsbekämpande myndigheter tillgång till sina användares kommunikation, inklusive sådan som är krypterad från slutpunkt till slutpunkt.² Det kommer att vara omöjligt att uppfylla detta krav för krypterade kommunikationstjänster från slutpunkt till slutpunkt utan att tvinga leverantörerna att skapa en bakdörr för kryptering. Vi inser vikten av att bekämpa olaglig verksamhet, men vi uppmanar starkt till försiktighet när det gäller åtgärder som skulle kunna undergräva krypteringens säkerhet och integritet, eftersom sådana åtgärder medför betydande risker för integriteten, cybersäkerheten och den ekonomiska konkurrenskraften. Detta skulle skapa ett aldrig tidigare skådat brott mot end-to-end-krypteringstekniken, som både stater och illvilliga aktörer skulle kunna utnyttja. En sådan åtgärd är extremt farlig. Som många institutioner, däribland Försvarsmakten³ och [Europeiska dataskyddskommittén](#),⁴ har upprepat, skulle detta försvaga skyddsnivån för all kommunikation och hota sekretessen för all informationsutbyte.

¹ <https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2024/11/utkast-till-lagadsremiss-datalagring-och-tillgang-till-elektronisk-information/>

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

³ Angav att [åtkomstkrav i end-to-end-krypterad kommunikation] "inte kan uppfyllas utan att man inför sårbarheter och bakdörrar som tredje part kan utnyttja".

<https://regeringen.se/contentassets/e22f777eb1964c258c5d9a21adb6a355/forsvarsmakten.pdf>

⁴ De nya reglerna bör också tydligt tillåta användare att använda end-to-end-kryptering (utan "bakdörrar") för att skydda sin elektroniska kommunikation. Dekryptering, bakåtkompilering eller övervakning av kommunikation som skyddas av kryptering bör vara förbjudet. Yttrande 5/2016 från Europeiska datatillsynsmannen

App Associationens småföretagsmedlemmar både i och utanför Sverige vet att för att kunna konkurrera på konsument- och företagsmarknaderna måste de kunna begränsa åtkomsten till data till behöriga användare på ett tillförlitligt sätt, säkerställa att data förblir korrekta och oförändrade samt garantera att informationen är tillgänglig när behöriga användare behöver den. End-to-end-kryptering är ett viktigt verktyg för att skapa förtroende och säkerhet hos kunderna. Försök från regeringar, senast Sverige, att införa krav på bakdörrar i krypteringsalgoritmer undergräver dessa mål avsevärt.

App Association stöder fullt ut insatserna för att bekämpa organiserad brottslighet, men den för närvarande debatterade lagstiftningen kommer inte att bidra till att uppnå detta mål. Dess genomförande skulle allvarligt skada säkerheten och förtroendet inom den digitala ekonomin genom att skapa brister i algoritmer som kan användas för att äventyra datasekretess, integritet och åtkomstkrav.

Det är omöjligt att reservera säkerhetsbakdörrar endast för de "goda". Om det finns en dörr kan och kommer illvilliga aktörer att utnyttja den. Sveriges krav skulle skapa ett prejudikat för andra länder och regimer att kräva liknande tillgång till krypterade privata data, vilket ytterligare skulle minska medborgarnas integritet och säkerhet.

Den skada som införandet av denna nya lag skulle orsaka svenska och europeiska småföretag som bedriver innovation och konkurrerar inom den globala digitala ekonomin är inte hypotetisk. Ett tydligt exempel är de statliga krav som infördes på 1990-talet på bredbandsleverantörer att ge brottsbekämpande myndigheter tillgång till krypterad kommunikation i deras nätverk, vilket nyligen har lett till att den kinesiska hackergruppen Salt Typhoon har fått oöverträffad obehörig tillgång till stora mängder känslig data. Omfattningen av detta intrång i amerikanska telekommunikationsnätverk utreds fortfarande, men i nuläget verkar det som om Salt Typhoons åtkomst i princip var obegränsad. Denna pågående episod är ett bevis på att krav på obegränsad åtkomst via bakdörrar till krypterade enheter eller data under överföring kommer att leda till att åtkomsten utnyttjas av oönskade aktörer. Erfarenheterna från Salt Typhoon visar att en försvagad kryptering utsätter företag för fler intrång, vilket skapar en ännu större risk för dem som redan är marginaliserade.

Cyberattacker mot kritisk infrastruktur ökar både i frekvens och allvar, vilket gör behovet av den säkerhet som end-to-end-kryptering ger viktigare än någonsin. En obligatorisk försvagning av krypteringen skulle undergräva det erkännande som den svenska försvarsmakten gjorde i januari 2025, när den konstaterade att "landet utsätts för regelbundna cyberattacker".⁵

Genom att ålägga plattformar att i hemlighet äventyra sin säkerhet skulle riksdagen väcka allvarliga farhågor om säkerheten hos produkter som används i Sverige, vilket skulle leda till att investerare och konsumenterna ifrågasätter om deras produkter innehåller dolda säkerhetsbrister som ålagts av riksdagen och att våra medlemmar inte kan växa och skapa arbetstillfällen i Sverige.

⁵<https://www.forsvarsmakten.se/sv/aktuellt/2025/01/hybridoperationer-skador-sverige/>

Det prejudikat som riksdagen skulle skapa kan också tvinga vissa av våra medlemmar att överväga att dra sig tillbaka från den svenska marknaden för att undvika de ryktesrisker som är förknippade med att undergräva säkerheten hos deras egna produkter. Slutligen skulle antagandet av en sådan lagstiftning inte bara skada Sveriges ställning inom global säkerhets- och innovationspolitik ⁶, utan också signalera ett avsteg från landets ledande roll inom dessa områden.

Sverige har makten att skydda krypteringsstandarder och se till att de förblir tillräckligt starka för att skydda den digitala infrastrukturen utan att skapa luckor som äventyrar säkerheten. Vi begär därför att riksdagen röstar nej till lagförslaget och inleder en reviderad policyutvecklingsprocess för att säkerställa att end-to-end-kryptering stödjer Sveriges nationella och ekonomiska säkerhet. Vår gemenskap är fast besluten att delta i en sådan process och att i större utsträckning stödja politik som stärker säkerheten och innovationen samt Sveriges globala ledarskap.

Vänliga hälsningar,



Mike Sax
Grundare och ordförande

Brian Scarpelli
senior rådgivare för global politik

Maria Goikoetxea Gomez de Segura
Policyansvarig

⁶ Framför allt har Europeiska domstolen för Rights (ECtHR) has condemned governments requiring företag att lämna ut krypteringsnycklar som oproportionerliga åtgärder som bryter mot mänskliga rättigheter. [https://hudoc.echr.coe.int/eng/#/%22itemid%22:\[%22001-230854%22\]](https://hudoc.echr.coe.int/eng/#/%22itemid%22:[%22001-230854%22]).