The undersigned civil society organizations, companies, and cybersecurity experts, including members of the Global Encryption Coalition,[1] urgently call for the Swedish Riksdag to reject the legislation, "Ju2024/02286 Datalagring och åtkomst till elektronisk information."[2] This legislation, if enacted, would greatly undermine the security and privacy of Swedish citizens, companies, and institutions. Despite its intention of combating serious crime, the legislation presents a dangerous approach which would instead create vulnerabilities that criminals and other malicious actors could readily exploit. Compromising encryption would leave Sweden's citizens and institutions less safe than before.

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.[3] The consensus among cybersecurity experts is that complying with this requirement for end-to-end encrypted communications services will be impossible without forcing providers to create an encryption backdoor[4] —akin to a master key that unlocks every door in a building.

The creation of an encryption backdoor creates vulnerabilities that would leave Sweden less safe against cyber threats and foreign adversaries. This concern is echoed by the Swedish Armed Forces, which has stated that [access requirements in End-to-end encrypted communication] "cannot be fulfilled without introducing vulnerabilities and backdoors that third parties can exploit."[5]

If passed, the legislation leaves platforms offering end-to-end encrypted services with an impossible choice. They will either need to comply and undermine the security of their services, or they will be forced to leave the Swedish market. In either scenario, the result is less secure and private communications for the Swedish citizens, companies, and institutions who rely on these tools.[6] Over 40% of Swedish Internet users benefit directly from the security and privacy provided by end-to-end encrypted messaging services.[7]

---

[1] The Global Encryption Coalition is a group of over 400 organizations, companies and cybersecurity experts that promotes and defends encryption in key countries and multilateral fora where it is under threat. https://www.globalencryption.org/

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

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

[4] https://www.cl.cam.ac.uk/archive/rja14/Papers/doormats.pdf

[5] https://regeringen.se/contentassets/e22f777eb1964c258c5d9a21adb6a355/forsvarsmakten.pdf

[6] Recently, UK citizens lost the protection provided by Apple's end-to-end cloud service, after the UK government attempted to force Apple to build an encryption backdoor. https://www.eff.org/deeplinks/2025/02/cornered-uks-demand-encryption-backdoor-apple-turns-its-strongest-security-setting

[7] https://www.statista.com/forecasts/1348051/most-used-messenger-by-brand-in-sweden

Undermining the confidentiality of end-to-end encrypted services would have a particularly harmful impact on those already at most significant risk: journalists and activists who rely on secure communication to protect sources and organize safely, families and domestic violence survivors who use encryption to shield themselves from abuse,[8] LGBTQ+ individuals who depend on secure platforms for safety and community,[9] and many more who rely on the protection and privacy provided by end-to-end encrypted services. International human rights bodies, including the European Data Protection Board and European Court of Human Rights, have recognized the importance of end-to-end encryption to protect the right to privacy and to promote the exercise of other rights.[10,11]

Swedish companies, government services, and institutions all benefit from end-to-end encryption. The Swedish Armed Forces recognized this when they recently endorsed the use of Signal, an end-to-end encrypted messaging application, to protect the non-classified communications of national security professionals.[12] If the legislation passes, Signal has already indicated that they would choose to leave the Swedish market rather than comply.[13]

Ensuring the security and privacy of government officials and national security professionals is vital for helping prevent extortion or coercion attempts, which could lead to more significant national security damage. The Swedish Armed Forces have noted in January 2025 that "the country is subject to regular cyberattacks",[14] and in such an environment, ensuring Swedish citizens, companies, and institutions have access to uncompromised end-to-end encrypted communications is more vital than ever.

Weakening encryption would be akin to lowering defenses during heightened risk. Amid such national security challenges and the fallout of the Salt Typhoon hack,[15] the reliance

---

[8] https://www.internetsociety.org/wp-content/uploads/2021/05/NNEDV_Survivor_FactSheet-EN.pdf

[9] https://www.lgbttech.org/encryption-privacy-security

[10] In 2022, a joint opinion from the European Data Protection Board (and European Data Protection Supervisor noted that "encryption technologies contribute in a fundamental way to the respect for private life and confidentiality of communications, freedom of expression as well as to innovation and the growth of the digital economy.https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

[11] In February 2024, the European Court of Human Rights found that Russia's order issued to Telegram requiring it to disclose "technical information" including encryption keys breached human rights law, as it was not proportionatePodchasov v Russia [2024] ECHR 134 [79]: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]

[12] https://www.forsvarsmakten.se/sv/aktuellt/2025/02/forsvarsmakten-anvander-appen-signal-for-oppen-kommunikation-med-mobiltelefoner/

[13] https://cybernews.com/news/signal-sweden-encryption-backdoor-police/

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

[15] https://cyberscoop.com/salt-typhoon-us-government-jen-easterly-cisa/

by the Swedish government, citizens, and businesses on end-to-end encryption to keep themselves safe and secure has never been greater.

Rather than undermining encryption, the government should invest in and utilize modern investigative techniques that are targeted and do not compromise the security of all users. These include enhanced digital forensics, improved data analysis, and international cooperation.

End-to-end encryption is vital to protecting Sweden’s interests. In light of the severe risks to security, privacy, and human rights, we strongly urge the Riksdag to reject “Ju2024/02286 Datalagring och åtkomst till elektronisk information.” Passing this legislation would damage Sweden's cybersecurity, digital economy, and commitment to human rights. It would create a legacy of vulnerability that would persist for generations.

We implore you to protect Swedish citizens' communications and fundamental rights, safeguard Sweden's digital future, and prioritize policies that strengthen rather than weaken cybersecurity. Sweden's security, prosperity, and freedom depend on it.

Signatories

Organizations

Access Now

Africa Media and Information Technology Initiative (AfriMITI)

African Academic Network on Internet Policy

Assured AB

Betapersei, SC

Bits of Freedom

Center for the Study of Organized Hate (CSOH)

Centre for Democracy & Technology Europe

Character Works AB

Comunitatea Internet Association

Cyberstorm.global

Danes je nov dan, Inštitut za druga vprašanja

Dataföreningen västra (Swedish Computer Association)

Deutsche Vereinigung für Datenschutz e.V. (DVD)

DFRI (Föreningen för Digitala Fri- och Rättigheter)

Dispersion AB

Egyptian Initiative for Personal Rights (EIPR)

Electronic Frontier Finland - Effi ry

Electronic Frontier Foundation

Elektronisk Forpost Norge

Encryption Advocates Council

European Digital Rights (EDRi)

European Roma Rights Centre

European Sex Workers Rights Alliance (ESWA)

Fight for the Future

Freedom of the Press Foundation

Global Partners Digital

Homo Digitalis

How to know AB

Index on Censorship

Internet Society

Internet Society Benin Chapter (ISOC BENIN)

Internet Society Cameroon Chapter

Internet Society Capítulo Venezuela

Internet Society Catalan Chapter (ISOC-CAT)

Internet Society Chad chapter

Internet Society Comoros Chapter

Internet Society Dominican Republic Chapter

Internet Society Ecuador Chapter

Internet Society Ethiopia Chapter

Internet Society German Chapter ISOC.DE

Internet Society Ghana Chapter

Internet Society Guinea Chapter

Internet Society Mali Chapter

Internet Society Niger Chapter

Internet Society Norway Chapter

Internet Society Paraguay Chapter

Internet Society Portugal Chapter

Internet Society Puerto Rico Chapter

Internet Society Senegal Chapter

Internet Society Slovenia Chapter

Internet Society Sierra Leone Chapter

Internet Society Sweden Chapter

Internet Society Taiwan Taipei Chapter

Internet Society Togo Chapter

Internet Society Uruguay Chapter

Internet Society Zambia Chapter

IT-Pol Denmark

JCA-NET(Japan)

Kamratdataföreningen Konstellationen

LGBT Tech

Mozilla

MyData Sweden

Myntex

NetTek Ltd

Omnifi Foundation

OneMore Secure AB

Open Knowledge Sweden

Open Rights Group

OpenMedia

OSIRIS SEC AB, Security Installer

Peergos Ltd

Phoenix R&D GmbH

Politiscope

Proton

Privacy International

Privacy & Access Council of Canada

Quilibrium

Recurity Labs GmbH

SecureCom

SECURECRYPT

SHARE Foundation

SkypLabs

Statewatch

Surfshark

Swedish Network Users Society

Tech for Good Asia

The Cybersecurity Advisors Network (CyAN)

The Swedish Internet Foundation

The Tor Project

Thomson Reuters Holdings AB

Totalförsvarets Förvaltningsorganisation

Tuta Mail

Virtual School on Internet Governance

XPD AB

3 Steps Data

Individual Experts*

Anders Abel, Sustainsys AB

Jaak Akker, CISSP

Viktor Alakörkkö

Magnus Almgren, Chalmers University of Technology

Anders Alfredsson, Devies Cybersecurity+

Petrus Allberg, Truesec AB

Thomas Althoff, Mainloop

Jakob Andersson

Jan Andersson

Vivi Andersson, KTH Royal Institute of Technology

Jörgen Anger-Annell, IT-architect

Daniel Appelquist, W3C TAG Co-chair and OpenSSF Global Cybersecurity working group co-chair

Oscar Asterkrans, All Embedded AB

Johan Åtting, Cyberly

Per Axbom, Axbom Innovation AB

Pierre Bäckström, Seeyou AB / On1Call Support AB

Martin Bergling, RISE - Research Institutes of Sweden

Fredrik Björeman, Kodsnack

Carl Mikael Björn, Vivetuvida Sverige AB

Simon Blomsterlund, Critical Tech AB

Rikard Borginger, Region Kronoberg

Anders Boström, Net Insight

Simon Bouget, RISE Research Institutes of Sweden

Tobias Brox, Redpill Linpro

Carl Magnus Bruhner

Randy Bush, RGnet

Jon Callas, Indiana University

L. Jean Camp, Indiana U

Sofia Celi, Brave

Dr Duncan Campbell, University of Sussex, School of Law Politics and Socioogy,, Brighton, UK

Anders Darander

Per Darnell

Angelique Dawnbringer, Accigo AB

Lars Delhage, Nohup AB

Orr Dunkelman, University of Haifa

Javier Ruiz Diaz, Sussex Centre for Law and Technology (SCLT)

Sven Dietrich, City University of New York (CUNY)

Tobias Ekbom, F.d. styrelseledampt Defensor, patenterat deduplicering i kombination med source-side encryption. Arkitekt i cybersäkerhet.

Torbjörn Eklöv

Tony Eklund, ICA

Peter Eriksson, Noproduct AB

Pontus Engblom, pingdash AB

Nicola Fabiano, Studio Legale Fabiano

Stephen Farrell, Trinity College Dublin

Dr. Simone Fischer-Hübner, Professor at Karlstad University

Dr. Richard Forno, UMBC

Mikael Forsgren, Verified Global AB

Amir Gaber

Simson L. Garfinkel, Association for Computing Machinery

Marcus Glaad

Simon Gökstorp, KTH Royal Institute of Technology

Dr. Ian Goldberg, University of Waterloo

Dr. Christine Grosse, LTU

Niklas Gustafsson, DPO

Masayuki Hatta, Surugadai University

Richard Hagerwald, Lead Architect Digital Workplace

Jacob Hallén, Sekans AB

Ulf Hedlund

Leif Henriksson

Kent Illemann, illemann konsult ab

Dr. Leonardo Horn Iwaya, Karlstad University

Emil Jacobson

Prof. Dr.-Ing. Meiko Jensen, Karlstad University

Carl-Arne Johannesson, Secufor AB

Olle E. Johansson, Edvina AB

Simon Josefsson

Johan Kallum

Per Kangru

Samuel Kelemen, Principal Security Engineer at King

Staffan Kerker, Splisado AB

Gabriel Kihlman, ABC-Klubben

Agnieszka Kitkowska

Markus Küchler, Epiroc

Mikael Kullberg, Cat Herd AB

Håkan Kvarnström, Independent consultant

Susan Landau, Tufts University

Magnus Larsson, Gislovs IT support & consulting

Richard Levitte, OpenSSL Foundation

Andreas Lindegren, KTH Royal Institute of Technology

Andreas Lindh, Recurity Labs GmbH

Ragnar Lönn, Odd Parity AB

Jesper Lönnqvist

Anne-Marie Eklund Löwinder, Amelsec AB

Dr. Kaspar Rosager Ludvigsen, Durham University

Johan Lundberg

Viktor Lundberg, CISO

Martin Lundgren, University of Skövde

Jens M, West Code Solutions AB

Jesper Madsen, Orange Cyberdefense

Claes Magnusson, Malmö Yrkeshögskola

Christian Meiczinger, Clavister AB

Victor Morel, Chalmers University of Technology

Kathleen Moriarty, Security BiaS

Renzo Navas, IMT Atlantique

Karl Emil Nikka, Nikka Systems

Andreas Nilsson, KTH

Jan Nilsson, Karlstad University

Marcus Ofenhed, Condition Raise AB

Mats Hagberg Olsson, Senior Solutions Architect, EQ2 Technology AB

Joakim Östling

Patrik Östman, CISO

Jörg Alexander Pareigis, Karlstad University

Gustav Petersson

Ivan Pettersson, Cybersecurity evangelist, Arrow ECS sweden

Victor Pettersson, CISO, Sokigo

Fredrik Pettai

Riana Pfefferkorn, Stanford University

Tobias Pulls, Karlstad University

Dr Gnanajeyaraman Rajaram, Saveetha University

Jonas Rendahl - CISO

Francisco Blas Izquierdo Riera (klondike), KITS AB and Chalmers University of Technology and University of Gothenburg

Josef Rudenlöv, Senior Cyber Security Advisor, Valisecure

Jakob Schlyter, Kirei AB

Mikael Schriwer, Drivlinan AB

Rima Sghaier, Digital rights advocate (independent)

Dr Jessica Shurson, University of Sussex

Ann Singleton, University of Bristol (signed in a personal capacity)

Johnny Slätt, AE Security

Eugene H. Spafford, Purdue University, USA

Daniel Stenberg, the curl project, president of the European Open Source Academy

Mats Strålberg, Inforing AB

Magnus Ström

Daniel Sörlöv, Microsoft

Peter Sunde Kolmisoppi, ex The Pirate Bay/Wikileaks

Erik Svensson

Niklas Svensson CISSP

Carl Svensson

Johan Thelin, Koderize

Marco Tiloca, RISE Research Institutes of Sweden

Ulrich Wisser

Paul Wouters, IETF Security Area Director

Anna Louise Yngström Valdre, professor em Stockholm Univerity

Magnus Vallstedt, Urban Hippo AB

Mališa Vučinić, Inria

Dr. Karin Zackari, Lund University

Daniel Zappala, Brigham Young University

*Affiliations listed for identification purposes only