AMCHAM

AMERICAN CHAMBER OF COMMERCE IN SWEDEN

White Paper - Cloud Services

Box 190, SE-101 23 Stockholm, Sweden | Klarabergsviadukten 63, Stockholm, Sweden
Tel: +46 8 506 126 10 | Org. No. SE 8020171883
info@amcham.se *amcham.se*

I. Background

1. eSam Statement

eSamverkansprogrammet (eSam), is a Swedish governmental digitalization organization established in 2015.[1] It is comprised of 23 public sector agencies and the Swedish Association of Local Authorities and Regions (Sveriges Kommuner och Landsting; "SKL") that work together to facilitate the digitalization of the public sector.

Source: eSam

In October 2018, eSam issued a *Legal Statement on Disclosure and Cloud Services* (*eSam Legal Statement*)[2] that has given rise to misconceptions and uncertainty among public agencies and authorities, as well as concomitant delays in key public procurement projects intended to digitally transform critical public sector services.

Problematically, the eSam Legal Statement cited an example related to the CLOUD Act:

> … the regulation that provides that U.S. authorities must also be provided access to data stored abroad and that U.S. service providers for that reason cannot refuse to disclose such data. According to this regulation, confidential information may be disclosed even if the actual storage takes place within the EU's borders.

[1] eSamverkansprogrammet: http://www.esamverka.se/.

[2] Rättsligt uttalande om röjande och molntjänster (Swedish), October 2018. eSamverkansprogrammet stated that confidential information made technically available to a service provider is deemed to have been disclosed if, by reason of ownership or otherwise, the service provider is subject to the jurisdiction of another country under which the service provider may be required to provide the confidential information, without reference to an international legal treaty or other legal basis under Swedish law. http://www.esamverka.se/download/18.290a0225166bfafb714c0c7a/1542007824143/eSam%20-%20Rättsligt%20uttalande%20om%20röjande%20och%20molntjänster.pdf. eSam released a supplementary statement on September 20, 2019. http://www.esamverka.se/download/18.4c1250a116d1bb3a3f094fe1/1568977769756/Kompletterande%20info%20om%20molnfr%C3%A5gan.pdf

On September 30, 2019, Minister Anders Ygeman announced that the Swedish government would appoint a special investigator to investigate the conditions under which public sector entities may gain access to secure and cost-effective IT services. The investigator will, *inter alia*, submit proposals for more secure forms of coordinated state IT operations and clarify the legal criteria that must be met to safely use private providers of IT services.[3]

The assignments to survey and analyze the government's IT operations and the legal conditions surrounding them must be reported by the special investigator no later than August 31, 2020. The task of proposing more secure forms of coordinated state IT services must be reported no later than May 31, 2021.

The Government has also decided to extend the Swedish Social Insurance Agency's (Försäkringskassan) ongoing assignment to offer coordinated and secure state IT services until December 31, 2022.[4]

2. The CLOUD Act

In 1986, the United States Congress enacted the Stored Communications Act ("SCA")[5], which covers law enforcement access to electronic communications. In 2016, the U.S. government served Microsoft an SCA warrant approved by an independent judge, who had found probable cause to justify the government's request for a search for electronic data related to the commission of a crime. An appellate court held, for the first time since the SCA was enacted, that the SCA did not require Microsoft to disclose information in its custody and control that it had stored on a server in Ireland. Many other U.S. courts disagreed with this decision, and it was on appeal to the U.S. Supreme Court when Congress enacted the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") in March 2018, mooting the case.

The CLOUD Act aimed to ensure clarity, by restoring the widely accepted and long-standing understanding of U.S. law. Significantly, the Act did not change existing U.S. legal principles on government data access requests, but did clarify that communications service providers subject to U.S. jurisdiction must disclose data within the company's "possession, custody, or control", regardless of where the data is stored.

In other words, the Act makes explicit in U.S. law the established principle (longstanding in both the United States and in many foreign countries) that a company subject to U.S. jurisdiction may be required to produce data within its custody and control, regardless of where it chooses to store that data. This provision simply codifies what had been the law and practice prior to the 2016 Microsoft decision[6], and ensures that the United States remains in

[3] Myndigheternas it-drift ska bli säkrare och mer kostnadseffektiv (Swedish), September 2019 https://www.regeringen.se/pressmeddelanden/2019/09/myndigheternas-it-drift-ska-bli-sakrare-och-mer-kostnadseffektiv/.
[4] Ibid.
[5] Stored Wire and Electronic Communications and Transactional Records Access, United States Code, 18 U.S.C. 121 https://www.govinfo.gov/app/details/USCODE-2016-title18/USCODE-2016-title18-partI-chap121.
[6] Microsoft v. United States, 829 F.3d 197 (2d Cir. 2016).

compliance with its obligations under the Budapest Cybercrime Convention[7], which requires all member states to have the power to compel providers in their territory to disclose electronic data in their control, no matter where stored. *Accordingly, the CLOUD Act did not alter whether or not a provider is subject to U.S. jurisdiction, nor did it give U.S. law enforcement any new authority to acquire data.*[8]

What is more, the Act updates the legal framework for how law enforcement authorities may request electronic evidence needed to protect public safety from service providers while respecting privacy interests and sovereignty by authorizing the United States to enter into bilateral agreements to facilitate the ability of trusted foreign partners to attain the electronic evidence they need to combat serious crimes. To qualify under the Act, a partner country must adhere to baseline rule-of-law, privacy, and civil liberties protections. Through bilateral agreements, each country would agree to lower the legal barriers that prevent their communication service providers from complying with qualifying lawful orders for electronic data issued by the other country. By dropping legal barriers, each country could serve its legal process – like search warrants – directly on the providers of the other country, dramatically increasing speed and efficiency compared with existing methods of transferring electronic evidence.

On October 3, 2019, the U.S.-U.K. signed a Bilateral Data Access Agreement pursuant to the CLOUD Act.[9] Significantly, it includes a carveout for government to government requests for data.[10]

3. The Real Story

The CLOUD Act does not:

- Give U.S. law enforcement any new legal authority to acquire data.
- Give U.S. courts expanded jurisdiction over companies or change the requirement that the U.S. must have personal jurisdiction over a company to require the disclosure of information the company holds.
- Alter the fundamental constitutional and statutory requirements U.S. law enforcement must meet to obtain legal process for data.

---

[7] The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[8] *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, U.S. Department of Justice, April 2019 https://www.justice.gov/opa/pr/justice-department-announces-publication-white-paper-cloud-act.

[9] U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, U.S. Department of Justice, October 2019 https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

[10] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

- Alter or expand the historical scope of warrants issued under U.S. law. Indiscriminate or bulk data collection is not permitted.
- Change U.S. law or practice regarding the U.S. Department of Justice's previous position that prosecutors should seek data directly from the enterprise client, if practical, and if doing so will not compromise the investigation.

4. Misperceptions and Myths[11]

Myth: U.S. law enforcement authorities will have unfettered access to the contents of stored communications.

> **Fact**: The initiating procedure for government access to communications content is a search warrant, signed by an independent U.S. judge.

Myth: The CLOUD Act will be used by U.S. law enforcement to access data stored by U.S.-based cloud providers.

> **Fact**: The CLOUD Act applies to several categories of service providers if they are subject to jurisdiction in the United States, regardless of where they are based. The U.S. Department of Justice has adopted a policy of not seeking data from the service provider, however, unless seeking data from the enterprise customer would sacrifice the investigation.

Myth: The CLOUD Act allows for data access requests to be made on various grounds, including civil, administrative or commercial inquiries.

> **Fact**: Warrants obtained under the CLOUD Act can only be issued by U.S. courts in connection with the investigation of criminal activity.

Myth: The CLOUD Act can create conflicts of laws and does not provide for means of recourse.

> **Fact**: The CLOUD Act contains robust safeguards and, even in the absence of an Executive Agreement between the United States and a foreign country, it offers a common-law recourse on comity. In other words, the CLOUD Act does not require an executive agreement to be in place between the U.S. and a foreign country for a provider to be able to challenge legal process issued under the Act on grounds of international comity.

Myth: The CLOUD Act is a one-way street, enabling the U.S. to access EU citizens' data without reciprocal EU access to U.S. data.

[11] *The US CLOUD Act: Myths vs. Facts*, BSA - The Software Alliance, April 2019 https://www.bsa.org/files/policy-filings/04112019uscloudactmyth.pdf.

Fact: The CLOUD Act explicitly provides for bilateral executive agreements and makes provision for non-U.S. authorities to access content stored by U.S. companies subject to appropriate restrictions and safeguards.

II. Impact of the *eSam Legal Statement* on Innovation

Innovation in the public sector is dependent on access to cloud services that offer robust security, scalability, cutting-edge technology, and highly skilled support. Not surprisingly, misconceptions about law enforcement access to data stored on cloud services have adversely impacted public procurement of cloud services. At least one such tender explicitly states that the service provider cannot be subject to the CLOUD Act.[12]

September 12 Seminar

Leveraging cutting edge technology is critical to improve healthcare, foster Industry 4.0, deliver smart city solutions and more; cloud services are the backbone supporting this 21st-century innovation. Everything from the security of networks and personal computers, to AI, and autonomous driving rely on cloud services.

But the Swedish public sector risks falling behind when it comes to digitalization and reaping the benefits of digitalization because of misconceptions about the CLOUD Act. As a consequence, there are delays in critical public procurement projects that impact healthcare initiatives, transportation, and more.

On September 12, 2019, AmCham hosted a seminar that examined the potential of innovative cloud services for the public sector and how misinterpretations of the CLOUD Act are challenging the ability of the public sector to capitalize fully on the opportunities afforded by digitalization.

During the seminars two U.S. legal experts explained the process and noted that it is wildly unlikely that Swedish government data would be accessed given the many safeguards in place. To do so would require a criminal case, predicated on "probable cause" that a crime was committed. Prosecutors would then consult with International Affairs of the Department of Justice to make the case as to why this information would need to be obtained. In such a case, the U.S. government would generally seek a cooperative process instead. Should the matter proceed further, the request would then go before an independent judge for review. Finally, the U.S. service providers may challenge (quash or modify) any order based on a conflict of laws that would require them to violate the host country's law to comply with the search warrant.

[12] On April 9, 2019, Försäkringskassan (the Swedish Social Insurance Agency) released a tender for Cloud Services that specifically states that the service provider cannot be covered by the CLOUD Act. In their tender, section 2.3 Cloud service to which the contract relates, the recommendation follows: "The service provider shall ensure that neither the service provider nor any of the subcontractors are covered by the United States Clarification Lawful Overseas Use of Data Act (CLOUD Act) or any other equivalent act in any other country which authorizes to access confidential data contained in the cloud service."

The businesses on the panel highlighted the importance of dispelling the myths and misunderstandings around the CLOUD Act that are limiting the use of innovative technology and slowing down delivery on ambitious digitalization plans in Sweden.

III. The CLOUD Act: Process

In general, if a government wants access to data held by a company on behalf of an enterprise client, the company would expect that government to deal directly with that client.

There are well-established policies and practices, which make clear that companies will not provide access to client data stored outside the lawful jurisdiction of any government requesting such data, unless the request is made through internationally recognized legal channels such as mutual legal assistance treaties (MLATs).

The CLOUD Act establishes an additional legal channel by which governments could agree bilaterally on procedures and safeguards to handle lawful requests for data stored under each other's legal jurisdiction.

In the absence of such a bilateral agreement or other internationally recognized legal channels such as an existing MLAT, companies will continue to take appropriate steps to challenge requests for data stored outside a government's legal jurisdiction through judicial action or other means.[13]

IV. Legal Opinion

AmCham Sweden retained Synch Advokat AB to review the impact of the CLOUD Act in Sweden and to craft a memo presenting their findings.[14]

Synch Advokat AB found that nothing in current Swedish legislation explicitly forbids Swedish public sector entities from using cloud services from foreign service providers. The confusion surrounding the CLOUD Act appears unjustified and to some extent based on misunderstandings. The enactment of the CLOUD Act has not changed the existing legal situation with regards to U.S. law enforcements' authorization to access information stored by electronic communication providers. The authority for such government data access requests was unchanged by the CLOUD Act. The process by which law enforcement authorities may gain access to data is well-established and clearly defined. Moreover, such access requires U.S. law enforcement authorities to establish "probable cause".

[13] Source: IBM, *Government Data Access Requests and the CLOUD Act*, 2019.
[14] *The CLOUD Act: Its Meaning And Consequences,* American Chamber of Commerce in Sweden, https://www.amcham.se/newsarchive/2019/6/17/the-cloud-act-amp-its-implications-for-business.

V. Conclusion

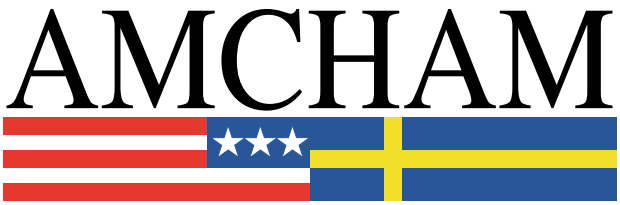
While the *eSam Legal Statement* has no binding effect and was arguably rendered moot by the Swedish Government's subsequent appointment of a special investigator to investigate public sector access to IT services, it has had a chilling effect on public procurement and, consequently, innovation in the public sector. At the same time there is an urgent need, and indeed a demand, within the public sector to use cloud services in order to digitally transform public services and operate as efficiently as possible.

Nothing in current Swedish law explicitly forbids public sector entities from using cloud services from foreign service providers. The enactment of the U.S. CLOUD Act does not make it more probable that information will be handed over to a third party. Instead, it clarifies long-standing U.S. law, establishes a transparent request process, and strengthens opportunities to challenge any request for access to data.

What is more, Sweden is in the process of ratifying the Budapest Cybercrime Convention[15], which obligates signatories to provide stored data from any legal entity or person in their territory. In fact, the European Union's proposed e-Evidence Regulation[16] would obligate every EU Member State to provide foreign-located evidence.

Finally, given the robust technical, statutory, and contractual protections available to customers, including individuals, enterprises, and the public sector, disclosure of protected data is unlikely. And it is wildly unlikely that the U.S. government would seek access to Swedish government data given the many safeguards in place and the historic and strong U.S. – Swedish relationship.

[15] Convention on Cybercrime, November 2001
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[16] E-evidence - cross-border access to electronic evidence, April 2018
https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en



AMERICAN CHAMBER OF COMMERCE IN SWEDEN

The Voice of American Business in Sweden

Box 190, SE-101 23 Stockholm, Sweden | Klarabergsviadukten 63, Stockholm, Sweden
Tel: +46 8 506 126 10 Org. No. SE 8020171883
info@amcham.se www.amcham.se