Memorandum
The Cloud Act

TO: American Chamber of Commerce in Sweden, ("AmCham")
FROM: Synch Advokat AB
RE: The Cloud Act
DATE: 14 June 2019

Table of content

Qualifications

We have been asked by the American Chamber of Commerce in Sweden ("AmCham") to prepare a memorandum on the CLOUD Act in order to explain and clarify the meaning and consequences of the same.

Because of the existing and relatively widespread misunderstandings and uncertainty about the current situation we have also been asked by Amcham to make our findings in this Memorandum public.

For these reasons we want to clarify and make the following qualifications. No person other than AmCham may seek to rely on the content of this memorandum for any purpose and we will not assume any duty of care, responsibility or liability to any other person in respect of this memorandum. We have prepared this Memorandum from the perspective of Swedish law only. Any matters that may be considered from the perspective of other laws have not been considered. Insofar as any such matters are referred to in this Memorandum, we do not therefore opine as to their legal effect.

We will not be responsible for advice or reports provided by any third party in connection with this Memorandum, irrespective of whether or not such advice or legal opinion is referred to or set out in this Memorandum.

This Memorandum is prepared on basis of the information available to us at the date hereof and no responsibility is undertaken by us to update this Memorandum by reference to information made available after the date of this Memorandum, or otherwise.

Executive summary

The digitalization in the public sector of Sweden has given rise to legal questions regarding under which circumstances authorities can use service providers without violating the applicable law of Sweden.

One of the main concerns among the authorities in Sweden has been regarding the Clarifying Lawful Overseas Use of Data Act (**"CLOUD Act"**), which allows U.S. law enforcement to request access to data from service providers subject to U.S. jurisdiction. This regardless of where the data is stored.

The U.S. Department of Justice (**"DoJ"**) explains in an April 2019 White Paper that the CLOUD Act does not expand the U.S. investigative authority nor does it extend the U.S. jurisdiction to any new parties, but merely serves to establish what has been long standing law in the U.S. The DoJ also points to the fact that the CLOUD Act is consistent with international principles regarding the fight on cybercrime.

In a legal statement published in October 2018, eSamverkansprogrammet (**"eSam"**) declared that confidential information made technically available to a service provider is deemed to have been disclosed[1] if, by reason of ownership or otherwise, the service provider is bound by rules in 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. The legal statement published by eSam in October 2018 differs significantly from a previous legal statement published by the same group in 2015 regarding information made technically available to a service provider.

The European Commission recognizes that more than half of all criminal investigations today require access to cross-border electronic evidence and that the U.S. is one of the main recipients of Mutual Legal Assistance Treaty (**"MLAT"**) requests from the EU. As the European Commission finds the MLAT process to be slow, initiatives have been taken to negotiate an agreement between the EU and the U.S. regarding cross-border access to electronic evidence for judicial cooperation in criminal matters.

We believe there are good reasons to challenge the legal statement published by eSam in October 2018, as this statement is too general and sweeping. The proper use of cloud services needs to be carefully analyzed on a case-by-case basis and we find support for the use of such services in applicable Swedish legislation (including GDPR) and case law.

1 Sw. "röjd".

Sammanfattning

Digitaliseringen i den offentliga sektorn i Sverige har gett upphov till ett flertal juridiska frågor beträffande under vilka omständigheter myndigheter kan använda sig av tjänsteleverantörer utan att bryta mot svensk lag.

En av de svenska myndigheternas farhågor har varit ikraftträdandet av lagstiftningen Clarifying Lawful Overseas Use of Data Act (**"CLOUD Act"**) i USA, vilken möjliggör att amerikanska rättsvårdande myndigheter har möjlighet att begära tillgång till uppgifter från tjänsteleverantörer som omfattas av amerikansk jurisdiktion, oavsett var uppgifterna är lagrade.

Det amerikanska justitiedepartementet (**"DoJ"**) förklarar i ett så kallat White Paper publicerat i april år 2019 att CLOUD Act inte utökar de befogenheter rättsvårdande myndigheter i USA har eller utökar den amerikanska jurisdiktionen till några ytterligare parter utan endast är ett klargörande avseende den lagstiftning i USA som varit tillämplig sedan lång tid tillbaka. DoJ hänvisar också till att CLOUD Act överensstämmer med internationella principer för att utreda cyberbrottslighet.

I ett rättsligt utlåtande som publicerades i oktober år 2018 förklarade eSamverkansprogrammet (**"eSam"**) att om sekretessreglerade uppgifter gjorts tekniskt tillgängliga för en tjänsteleverantör, ska uppgifterna anses ha röjts om tjänsteleverantören, på grund av sin ägarstruktur eller andra omständigheter, är bunden av regler i ett annat land enligt vilken tjänsteleverantören kan vara skyldig att tillhandahålla uppgifter, utan hänvisning till en internationell rättslig överenskommelse eller annan rättslig grund enligt svensk lag. Det rättsliga utlåtandet som publicerades av eSam i oktober år 2018 skiljer sig avsevärt från ett tidigare rättsligt utlåtande som publicerats av samma grupp år 2015, avseende information som gjorts tekniskt tillgänglig för en tjänsteleverantör.

Europeiska kommissionen uppskattar att mer än hälften av alla brottsutredningar idag kräver att elektroniska bevis inhämtas gränsöverskridande, och att USA är en av huvudmottagarna av ansökningar om att lämna ut sådana elektroniska bevis (**"MLAT"**) till EU. Eftersom Europeiska kommissionen finner MLAT-processen långsam har initiativ tagits till att förhandla fram ett avtal mellan EU och USA om gränsöverskridande tillgång till elektroniska bevis för att förenkla brottsutredande samarbeten.

Vi anser att det finns goda skäl för att ifrågasätta eSams rättsliga utlåtande från oktober år 2018, eftersom utlåtandet i fråga bygger på, vad vi anser vara, vag och allmänt hållen argumentation. Korrekt användning av molntjänster måste analyseras noggrant och vi finner stöd för användningen av sådana tjänster enligt tillämplig svensk lagstiftning (vilket inbegriper GDPR) och rättspraxis.

1. Introduction

We are rapidly moving into a new era of technology where digitization and digital transformation is at the top of every organization's agenda, private or public.

The public sector is tasked by the Swedish government with carrying out its business in an efficient way and always act responsibly with given resources. As part of this task, public sector entities have evaluated the activities they perform and which of them they should continue to carry out internally and which they should contract out.

Functions such as IT-based storage, document management and email are fundamental for an authority to carry out its daily operations in an effective manner. Today, both private and public sector entities make use of a variety of on-premise solutions, outsourcing solutions as well as cloud solutions. Due to the continued need of more efficient, secure and modern IT-based support for organizations, the expectation is that the shift to cloud services will increase and this is also a trend among service providers and their customers.

The importance of entering the digital era is further emphasized in Sweden through various initiatives and not least through the creation of a specific authority for these purposes; the Agency for Digital Government ("**DIGG**"). On DIGG's website it is stated that:

"Digitalization fundamentally changes our society. It affects how we live and how we work – and it provides opportunities to do things we have never done before.

Sweden has the goal of being the best in the world at leveraging the potential of digitalization. An efficient and innovative public sector is of great importance to Sweden.

We at DIGG are a catalyst for digitalization of the public sector."[2]

In recent years we have seen a number of relevant laws and regulations coming into effect which all have bearing on data, the use and transfer of the same, e.g. the General Data Protection Regulation ("**GDPR**")[3], the NIS Directive[4], the Swedish Protective Security Act[5] and the CLOUD Act.[6]

[2] https://www.digg.se/about-us/public-sector-digitalization (collected 26 May 2019).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[5] The Swedish Protective Security Act (SFS 2018:585).
[6] Consolidated Appropriations Act, Pub. L. No. 115-141, §§ 101–106, 132 Stat 348, 1213–25 (23 March 2018).

eSam, which is a collaboration program among 23 Swedish authorities and the Swedish Municipalities and County Council ("**SKL**") with the purpose to take advantage of the opportunities of digitization and use resources in an efficient manner, has issued statements with regards to outsourcing as well as to the use of cloud services. These have unfortunately increased the uncertainty amongst the public sector entities and caused widespread confusion and misunderstanding regarding the CLOUD Act and the possibility for public sector entities to securely use cloud services.[7]

In this Memorandum, we will briefly describe the content of eSam's statements as well as the CLOUD Act, including the White Paper published in April 2019 by the DoJ regarding the CLOUD Act.[8] Furthermore, we will analyze the definition of disclosure in applicable Swedish legislation and whether the legal statement from eSam published in October 2018 regarding confidential information in connection with the use of certain types of cloud services is aligned with the definition of disclosure in the abovementioned legislation.

The overall aim of this Memorandum is to assess whether the concerns raised by some Swedish public sector entities regarding the usage of a service provider bound by rules in another country under which the service provider may be required to provide data, without reference to an international legal treaty or other legal basis under Swedish law, are justified or not.

[7] Kammarkollegiet, Förstudierapport Webbaserat kontorsstöd, p. 6.
[8] Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, US Department of Justice, April 2019.

2. Esam Statements

In October 2018, eSam published a legal statement on confidential information in connection with the use of certain types of cloud services ("eSam Cloud Statement")[9].

It should first be noted that statements from eSam have no specific legal status and should merely be considered as recommendations or guidelines without being binding upon its members or any third party.

In the eSam Cloud Statement the legal expert group 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 bound by rules in 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.[10]

The opinion of the expert group is based on the view that it is no longer unlikely that confidential information submitted to such service provider may be disclosed to a third party. In addition, eSam is of the opinion that confidential information, which is made technically available to a service provider, is deemed to be disclosed if it is suspected that the ownership or the service provider's geographical location would mean that human rights or the public interest of Sweden would not be ensured if the Swedish authorities' confidential information had been made available to the service provider.[11]

The eSam Cloud Statement differs significantly from a previous legal statement made by the same group in 2015 regarding information made technically available to a service provider,(**"eSam Outsourcing Statement"**)[12]. According to this statement, eSam made it clear that when information is made technically available through outsourcing to a service provider, there is no intention that the service provider interpret the information made available. Instead, the purpose is solely that the service provider shall technically process or store the information. Based on this, eSam concluded that when an authority is outsourcing certain functions, e.g. IT outsourcing, a disclosure shall not exist according to the Public Access to Information and Secrecy Act[13] ("OSL") as long as the service provider is not allowed to interpret or forward the information, and the circumstances otherwise indicates that this is unlikely to happen.[14]

[9] Rättsligt uttalande om röjande och molntjänster, eSam, 23 oktober 2018.
[10] Op. cit. 1.
[11] Op. cit. 2.
[12] Outsourcing – en vägledning om sekretess och persondataskydd, eSam.
[13] The Public Access to Information and Secrecy Act (2009:400).
[14] Rättsligt uttalande om röjandebegreppet i offentlighets- och sekretesslagen, eSam, p. 1. 15 Outsourcing – en vägledning om sekretess och persondataskydd, p. 18-19.

In the eSam Outsourcing Statement, eSam also refers to a guidance document drafted by the expert group for further information on the subject. In the guidance document, eSam clarify a few prerequisites that must be in place for an authority to outsource its IT function. The authority shall:

- contractually prohibit the service provider to interpret or share any information made available by the authority;
- ensure that measures are in place to verify the service provider's compliance with the contract; and
- prescribe significant sanctions upon the service provider in case of breach of contract.

Under the abovementioned circumstances, eSam finds, according to the guidance document, that it would be unlikely that the service provider or any unauthorized person would interpret or forward the information made available by the authority and therefore no disclosure would be present according to the OSL.[15]

[15] Outsourcing – en vägledning om sekretess och persondataskydd, p. 18-19.

3. The Cloud Act

The CLOUD Act was signed into law March 23rd, 2018 and amends the U.S Stored Communications Act[16] ("SCA").

The reason for the introduction was to clarify the specific judicial mechanism that U.S. law enforcement can use pursuant to the SCA to seek access to information held outside the United States if such information was used to commit a crime under U.S. law. The CLOUD Act allows U.S. law enforcement authorities to access "the contents of a wire or electronic communication and any record or other information" about an individual, regardless of where the individual is a resident or where the information is stored, from any electronic communication provider.[17] The CLOUD Act may result in that data stored in the EU will be disclosed to U.S. authorities and under certain circumstances, the CLOUD Act also allows foreign governments to request data stored in the U.S. or by a service provider under U.S jurisdiction.

The CLOUD Act was implemented as a consequence of a dispute between Microsoft and the U.S. government regarding the scope of the SCA.[18] The core of the dispute consisted of the U.S. Government considering that they had the right to request information from a business (e.g. Microsoft) regardless of where the data was stored. Microsoft contested this and argued that the U.S. government could only request data stored in the U.S. Furthermore, Microsoft stated that if the U.S. government wanted access to data stored in another country, the U.S. Government needed to enter into a MLAT with the foreign government in question. In the Microsoft case, the EU Commission drafted an amicus curiae statement, which concluded, in summary, that the EU has an interest in international cooperation regarding justice matters, but that any form of disclosure of data stored in the EU must be done in accordance with the GDPR in order to be legal.[19] The case between Microsoft and the U.S. government was vacated as the CLOUD Act was introduced.

It should be noted that the CLOUD Act also provides a mechanism for the implementation of bilateral agreements between the U.S. and the governments of other countries (as further described in section 5.1. below). Section 105 of the CLOUD Act stipulates that the U.S. may conclude an executive agreement with a foreign government on access to data, provided that the foreign government complies with a list of requirements regarding integrity and human rights.[20]

[16] 18 U.S. Code Chapter 121 §§ 2701–2712.
[17] CLOUD Act, § 2713 Code of Laws of the United States of America.
[18] United States of America v. Microsoft Corporation (04/17/2018).
[19] United States of America v. Microsoft Corporation, No 17-2, p. 2 f.
[20] CLOUD Act, § 2523 Code of Laws of the United States of America.

4. U.S. Department of Justice White Paper

4.1 The purpose of CLOUD Act

As the CLOUD Act was only intended to clarify the already existing legal situation and process to be used by U.S. law enforcement, the U.S. Department of Justice (**"DoJ"**), has published a White Paper to further explain the situation. The U.S. government enacted the CLOUD Act as a reaction to foreign partners expressing concerns that the MLAT was slow and burdensome. In order to ensure efficient access to electronic information held by U.S.-based service providers upon request by third countries investigating serious crime, the CLOUD Act was created to enable electronic evidence to be provided in a timely matter.[21]

The DoJ emphasizes that the CLOUD Act has two distinct parts. The first part addresses "CLOUD Act Executive Agreements" which authorizes the U.S. government to enter into executive agreements with foreign states under which the parties to such agreement will remove any legal barriers that may prohibit compliance with a competent court order issued in the respective party's country. By entering into a CLOUD Act Executive Agreement, the ambition is to enable the parties to submit orders for electronic evidence upon investigation of serious crime within the respective jurisdiction without any potential conflict of laws. The abovementioned agreements require that each party commit to significant provisions e.g. regarding privacy and civil liberties.22 It should be noted that Sweden, as of the date of the publication of this Memorandum, has not signed such Executive Agreement with the U.S. , and to our knowledge, no other country has either.

The second part of the CLOUD Act concerns "Ensuring Lawful Access to Data" which clarifies existing U.S. law that service providers, subject to U.S. jurisdiction, must disclose data requested in a valid U.S. legal process regardless of where the service provider stores the data.

The DoJ explains that the CLOUD Act complies with the Budapest Convention and does not expand the U.S. investigative authority nor extend the U.S. jurisdiction to any new parties but is merely restoring a widely accepted and long-standing understanding of the U.S. law.[23]

[21] U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, p. 2.
[22] Op. cit. 4.
[23] Op. cit. 6.

In the conclusion of the White Paper, the DoJ explains that the CLOUD Act was a necessity to address the problems arising from global companies operating storage centers in multiple countries, which also includes daily transfers between servers in different countries (e.g. leading to uncertainty regarding where the data is stored and MLAT requests to multiple governments). In order to mitigate the adverse effects on the foreign partners of the U.S. investigating serious crime, the CLOUD Act will support countries in protecting their societies and keeping their citizens safe.[24]

4.2 The request for information procedure

A U.S. government entity can request information from a provider of electronic communications in two ways. First off, the government entity can obtain a warrant issued in accordance with the Federal Rules of Criminal Procedure by a court of competent jurisdiction. Secondly, a governmental entity can request information from a provider using either an administrative or grand jury subpoena or a court order. In case of warrants, the government entity can obtain the content of the electronic communications without notice to the subscriber or customer of the service provider.[25]

In order for a government entity to obtain a warrant in the abovementioned situation, the targeted provider must be a provider of either Remote Communication Services or Electronic Communication Services. Furthermore, the provider must be under the jurisdiction of the U.S. court and the evidence sought must be in the possession, custody or control of the provider. In order to be able to issue a warrant, U.S. Law enforcement must abide by legal process (which includes the establishment of "probable cause" for the content in question) and the warrant may not violate principles established in prior U.S. case law.[26] Probable cause is only present if (a) a reasonable person would find sufficient evidence that a crime has been committed and (b) the evidence held by the service provider is relevant to the investigation of the crime.[27]

Upon receipt of a warrant, the service provider may challenge the warrant for a host of reasons. The CLOUD Act in particular prescribes that the service provider may challenge or quash the warrant if the service provider believes that:

- the customer or subscriber in scope of the warrant is not a U.S. person and does not reside in the U.S; and
- the required disclosure would create a material risk that the service provider would violate the laws of a qualifying foreign government.[28]

Despite the possibility to request the information from the service provider, in a guidance document from 2017 published by the DoJ, U.S. prosecutors are recommen-

[24] Op. cit. 7-8.
[25] 18 U.S. Code § 2703.
[26] E.g. Société Nationale Industrielle Aérospatiale, 482 U.S. at 544 n.28 (1987).
[27] Siegel, L & Worrall, J, Introduction to Criminal Justice, p. 297.
[28] CLOUD Act § 103 (a)(1).

ded to seek data directly from the enterprise rather than from its cloud-storage provider (if practical and given that doing so will not compromise the investigation).[29] But if the request is directed to the service provider and the service provider chooses to challenge or quash the warrant, the requesting governmental entity must respond to such action first and thereafter may the court modify or quash the legal process as appropriate. The global providers, such as Microsoft, Google and AWS, are fully aware of the possibility to challenge a request for customer information from a U.S. government entity and have a history of challenging such requests and will continue to do so.[30]

The CLOUD Act is so called "encryption neutral" and does not create any new authority for U.S. law enforcement to compel a service provider to break the encryption of the communications. Also, the CLOUD Act neither prevent a service provider from assisting the customer to encrypt its information nor put restrictions on foreign countries to have their own rules regarding decryption in domestic law.[31]

[29] U.S. Department of Justice, Seeking Enterprise Customer Data Held By Cloud Service Providers.

[30] The CLOUD Act is an important step forward, but now more steps need to follow, Brad Smith, 3 April 2019, https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/ (collected 26 May) and Clarifying Lawful Overseas Use of Data (CLOUD) Act, Amazon, https://aws.amazon.com/compliance/cloud-act/ (collected 26 May 2019).

[31] U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, p. 18.

5. ”Disclosure”under the OSL

5.1 When information is considered to be disclosed

The Swedish authorities' handling of confidential information is regulated by the OSL. Today, several government representatives state that there is uncertainty regarding how the definition of disclosure in the applicable confidentiality legislation should be interpreted.[32]

The definition of disclosure was unfortunately not discussed in the preparatory work of the OSL. Some guidance could possibly be found in the preparatory work for the Secrecy Act (1980:100) (which is now repealed and replaced by the OSL) as there is nothing in the OSL or its preparatory works indicating that a change is intended. There, a disclosure is defined as i) when a government official allows someone to access confidential information, whether in a public document, (ii) that someone may access parts of a document that is not public, or (iii) that confidential information is provided in a letter. The definition is not exhaustive and the legislator states that all forms of disclosure are covered, even when someone, for example, shows a secret object to someone else. It does not matter if the confidential information is provided on request by the third party or on the initiative of the person holding the confidential information.[33]

Furthermore, in a ruling from 1991, the Swedish Supreme Court (”HD”) analyses the definition of disclosure in relation to the provision on negligence with confidential confirmation in the Swedish Penal Code[34] (”BrB”) chapter 19, section 9. Although the ruling relates to criminal law, the legal doctrine is of the opinion that the analysis from HD can be used when interpreting the definition of disclosure in the OSL[35]. In the ruling, HD initially states that the term ”disclosing information” according to common language means that confidential information is disclosed or revealed and that it requires that there is a person, for whom the confidential information is made available. However, HD continues and clarifies that it should not always be required that such a person has become aware of the confidential information and that it can usually be enough for the confidential information to come into the possession of an unauthorized person. In conclusion, HD finds that any possibility for an unauthori-

[32] SOU 2018:25, Juridik som stöd för förvaltningens digitalisering, p. 339.
[33] Prop. 1981/82:186, om ändring i sekretesslagen m.m. p. 119 f.
[34] The Swedish Penal Code, sw. Brottsbalken (1962:700).
[35] Offentlighets- och sekretesslagen. En kommentar, kommentaren till 3 kap § 1, Lenberg m.fl.

zed person to access confidential information cannot cause the confidential information to be deemed disclosed. Instead, HD is of the opinion that it is crucial if the confidential information is made available to an unauthorized person under such circumstances that one must expect that the unauthorized person will interpret the confidential information.[36]

The primary difference between the interpretations under the previously applicable Secrecy Act and the analysis made by HD is that the Secrecy Act presupposed that someone access the confidential information, which is different from the HD-case. Worth taking into account is also that the legislator in the preparatory work of the Secrecy Act stated that some room for interpretation must exist regarding the definition of disclosure, in order to allow for flexibility in determining when criminal liability for disclosing confidential information occurs. The legislator states that misjudgments in difficult cases will generally be penal-free and that typical examples of intent will be present e.g. when confidential information is disclosed in violation of the Secrecy Act to the mass media.[37]

If we allow ourselves to take guidance on the definition of disclosure from the previously applicable Secrecy Act's and apply it to the situation when an authority make confidential information technically available to a service provider which, by reason of ownership or otherwise, is bound by rules in 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, a disclosure will only exist when (i) the service provider has disclosed the information to a third party and (ii) the third party either access the confidential information or understands that the information is confidential.

[36] NJA 1991 s. 103.
[37] Prop. 1981/82:186, om ändring i sekretesslagen m.m. p. 85.

5.2 Disclosure by act of storage

In light of the definition of disclosure in the Secrecy Act and the judgement from HD, we question how only the act of storage by means of a service provider can constitute a disclosure. We also believe that if the confidential information in question is encrypted, neither the service provider nor the third party can access the confidential information or understand that the information is confidential, which according to the previously applicable Secrecy Act's is a requirement for a disclosure to exist. Due to the fact that the legislator did not discuss the concept of disclosure when introducing the OSL, it is justified to assume that the definition in the previously applicable Secrecy Act's also applies regarding the OSL. Our overall assessment is therefore that eSam's current interpretation of disclosure extends beyond the definition of disclosure in the Swedish applicable legislation regarding confidentiality.

If we instead use the interpretation made by HD and apply it to the situation when an authority make confidential information technically available to a service provider which, by reason of ownership or otherwise, is bound by rules in 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, a disclosure will only exist when (i) the confidential information has been made available to an unauthorized person and (ii) the circumstances under which the confidential information is made available are such that one must expect that the unauthorized person will interpret the confidential information. Also, in this situation we question whether the interpretation of HD could be used to support the opinion that the mere act of storage by means of a service provider can constitute a disclosure. However, the interpretation of HD allows for a greater possibility to argue that a disclosure to an unauthorized person could exist even if the confidential information in question is encrypted. This is because one can expect in some cases that an unauthorized person, to whom the encrypted confidential information is made available, has the competence to break the encryption (for example, the intelligence service of a foreign country). However, like our analysis of the interpretation of disclosure under the applicable confidentiality legislation, we find that eSam's current interpretation of disclosure does not conform with the definition of disclosure in Swedish case law.

6. Third Country Request of Personal Data under the GDPR

Since the GDPR is applicable law in Sweden, it is necessary to discuss whether a transfer of personal data upon request by a third country may be considered a violation of the GDPR.

This will mainly be relevant if an authority in Sweden is making personal data technically available to a service provider which, by reason of ownership or otherwise, is bound by rules in another country under which the service provider may be required to provide the personal data, without reference to an international legal treaty or other legal basis under Swedish law.

According to article 48 of the GDPR, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a MLAT, in force between the requesting third country and the European Union or a Member State, without prejudice to other grounds for transfer pursuant to Chapter V of the GDPR.

Other grounds for transfer pursuant to chapter V can be found in article 49 of the GDPR. The European Data Protection Board (**"EDPB"**) has in their guideline from 2018 stated that article 49 (e) of the GDPR can cover a range of activities, such as criminal and administrative investigations in a third country.[38] This view is also supported by recital 115 of the GDPR which prescribes that transfers of personal data, as a result of extraterritorial application of non-member state law, should only be allowed where the conditions of the GDPR for a transfer to third countries are met, which would be the case, inter alia, where disclosure is necessary for an important ground of public interest recognized in Union or Member State law to which the controller is subject.

Therefore, even if it seems preferable according to the provisions of the GDPR that a transfer of personal data upon request of a third country is subject to an international agreement, alternative grounds for such transfer seem to exist. To summarize, it is not automatically a violation of the GDPR to transfer personal data upon request by a third country, as long as a ground for such transfer exists in chapter V of the GDPR.

[38] European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 11.

7. Current Legislative Process in the EU

The European Commission recognizes that more than half of all criminal investigations today require access to cross-border electronic evidence and that the U.S. is one of the main recipients of MLAT requests from the EU.

As the European Commission finds the MLAT process slow, initiatives have been taken to negotiate an agreement between the EU and the U.S. regarding cross-border access to electronic evidence for judicial cooperation in criminal matters.[39]

The initiative is part of the European Commission's proposal to the European Parliament and the Council regarding a Regulation on European Production and Preservation orders for electronic evidence in criminal matters and a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (**"E-evidence proposals"**).[40]

The initiative aims to address the legal issues of access to data held by service providers in the EU or the U.S and would complement the E-evidence proposals by addressing conflicts of law and speeding up access to electronic evidence (e.g. by enabling direct cooperation with a service provider). The European Commission stresses that the EU has an interest in a comprehensive agreement with the U.S. in order to protect human rights in the EU and the security of the Union.[41]

To this date, no such agreement has come in force.

[39] COM (2019) 70 final, p. 1-2.
[40] Op. Cit. 3.
[41] Op. Cit. 4.

8. Conclusion

As previously mentioned, there is a willingness and pressing need in the public sector to be able to use cloud services in order to operate as efficiently as possible.

Furthermore, with more and more service offerings becoming cloud based there is an urgent need to clarify under which circumstances a public authority can use cloud services without violating applicable laws in Sweden.

In our opinion nothing in the current Swedish legislation explicitly forbids Swedish public sector entities from using cloud services, even from foreign service providers.

The controversy surrounding the CLOUD Act, according to our analysis, 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' rights to access information stored by electronic communication providers. Such rights are clearly defined and require the U.S. law enforcement to establish "probable cause" and remain unchanged by the introduction of the CLOUD Act.

For some reason, the introduction of the CLOUD Act has been taken as reason to question of when and how Swedish public sector entities may use cloud services from service providers with a connection to the U.S.

The conclusions in the eSam Outsourcing Statement and the eSam Cloud Statement respectively are very different. In the eSam Outsourcing Statement the expert group has reached the same conclusions as we have, namely that there must exist a possibility to contract out certain activities without this being automatically deemed to be a disclosure. This assumes that the service provider, who receives technical access to the information, is contractually bound not to interpret and/or disclose the information and the circumstances are such that this would seem improbable.

eSam's conclusion in the eSam Outsourcing Statement finds its legal support in the preparatory works of the Secrecy Act (preceding the OSL) and certain case law from HD. It would have seemed reasonable to apply the same reasoning and methodology for cloud services as for outsourcing services. However, in the later statement from eSam, the eSam Cloud Statement, the conclusion is different and the argument provided is that "…it is no longer improbable that the information will be handed over to a third party."

39 COM (2019) 70 final, p. 1-2. 40 Op. Cit. 3.
41 Op. Cit. 4.

eSam does not provide much more support for having reached a different conclusion other than that cloud services generally (i) are using servers in different countries, (ii) content may be mirrored on servers in different countries, (iii) can be moved quickly between servers, and (iv) be accessed through networks. It may be true that cloud services are more agile than traditional outsourcing services which eSam had in mind for the eSam Outsourcing Statement, but it must be questioned whether this is really sufficient for reaching a different conclusion. Furthermore, it is unclear what the position would be if none of these or only one or two of these factors were present for a specific cloud service provider.

As the CLOUD Act hasn't changed the rights for U.S. law enforcement and traditional outsourcing service providers are covered by the long standing SCA it is difficult to see how eSam's two statements can be compatible. The enactment of the CLOUD Act does not make it more probable that information will be handed over to a third party but rather clarifies long standing law in the U.S., establishes a transparent request process and improves the possibilities to challenge a request for access to data from the U.S. government. As a side note, and as many of the larger U.S. cloud service providers transparently report the access requests, we have not been able to find a single instance where, under the SCA (both before and after the enactment of the CLOUD Act) they have been asked to hand over information owned by Swedish public sector entities. In addition, the CLOUD Act does not violate the Budapest Convention on Cybercrime, which Sweden has also signed but not ratified.[42]

To summarize we therefore consider it justified from a practical, but also from a legal perspective, that Swedish authorities use cloud services in their daily activities. However, such use should of course be subject to continuous documentation and appropriate technical and organizational measures, as in all outsourcing situations. Our hope is that the general discussion about the use of cloud services will mature since the use of cloud services can be of great benefit to the societies around the world.

However, there is a need to make an assessment on a case by case basis, where a number of items need to be carefully determined, e.g. type and category of data, the means of transfer and commercial terms for this.

As a general rule of thumb, we propose the following recommendations:

- For information that is to be kept secret under the OSL there should be a possibility to use cloud services provided that one:

  - contractually prohibits the cloud service provider to interpret or share any information made available by the authority;
  - ensures that measures are in place to verify the cloud service provider's compliance with the contract; and
  - prescribes significant sanctions upon the cloud service provider in case of breach of contract.

- For information that is to be kept secret under the higher security classes outlined in the Protective Security Act we believe that there may be difficulties in satisfying the requirements as set out in the Act, but it shouldn't be completely ruled out.

[42] The Budapest Convention on Cybercrime.