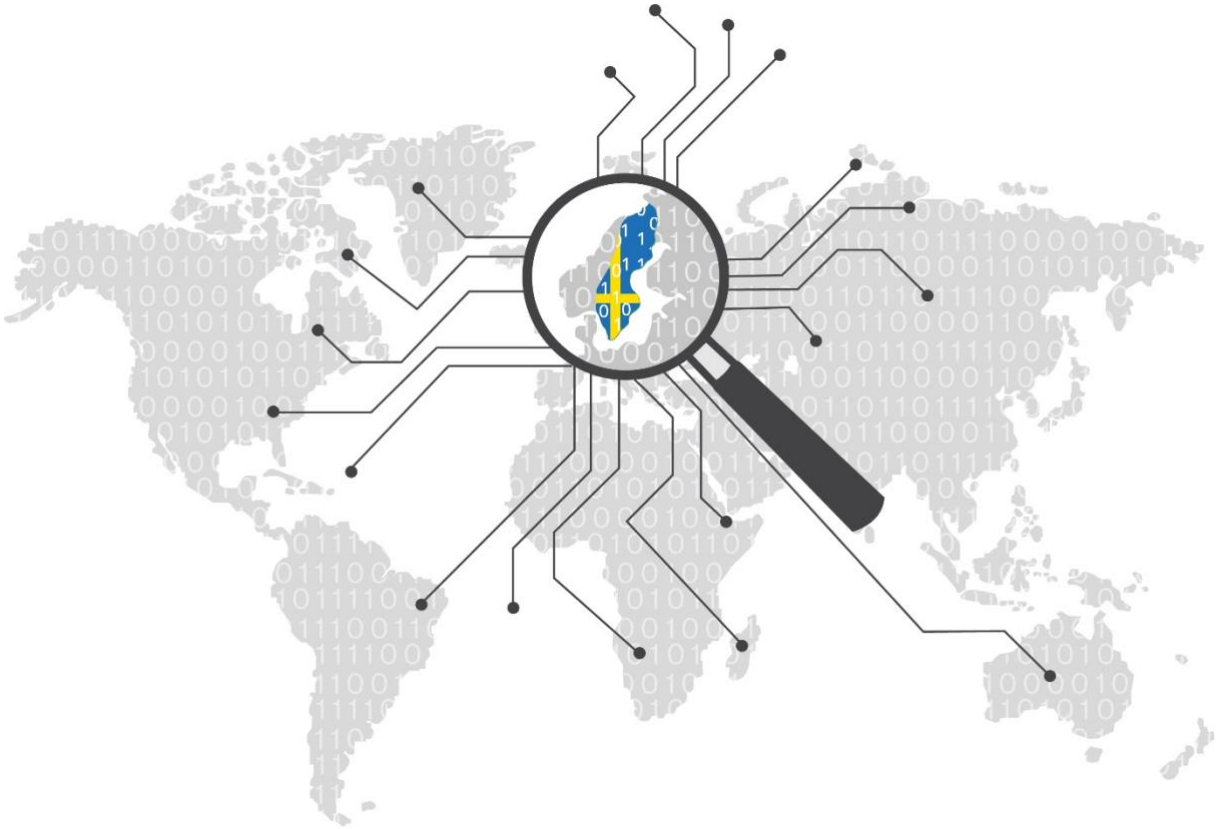

White Paper

Cloud Services in Sustaining Societal Functions – Risks, Appropriateness and the Way Forward

Försäkringskassan

White Paper – Cloud Services in Sustaining Societal Functions – Risks, Appropriateness and the Way Forward; Swedish Social Insurance Agency reference number: 013428-2019

Version: 1.0

Date: 18-11-2019

Like many other governmental agencies, the Swedish Social Insurance Agency offers easier access to information and services and streamlines internal processes with the aid of digital services. Cloud services offer good functionality, operational reliability and technological security at a reasonable cost. It is desirable and to a certain extent necessary for the public sector to be able to benefit from this.

At the same time, we cannot ignore the increasing vulnerability that digitalisation of sustaining societal services entails. Sweden's digital sovereignty must be ensured and the public administration must retain or take back control of sustaining societal digital services and data.

The decisions that are taken now will set the boundaries for our room to manoeuvre for the foreseeable future and influence Sweden's capacity to meet future challenges. The choice of IT services in sustaining societal activities will have consequences for citizens, individual agencies and the government administration as a whole, as well as Sweden as a state.

The Swedish Social Insurance Agency's increasing dependency on secure, user-friendly and robust digital services requires the agency to determine if and when it is appropriate and feasible to use public cloud services that are offered by private suppliers. This decision is based on our responsibility and obligation to frequently handle highly sensitive confidential data about private individuals as securely as possible. Although the analysis in this White Paper is based on the Swedish Social Insurance Agency's operations, our hope is that it may also be a tool for others making strategic decisions related to digitalisation and IT.

The White Paper was signed off by Director General Nils Öberg in the presence of Deputy Director General Maria Rydbeck, IT Director Stefan Olowsson and Chief Legal Counsel Mikael Westberg after presentation by Digital Strategist Anna Fors and Legal Expert Nina Stierna.

Anna Fors
Digital Strategist

Nina Stierna
Legal Expert

Contents

Annexes:

Summary

Like many other governmental agencies, the Swedish Social Insurance Agency benefits from using 'cloud services'. In many cases these services have led to better access, operational benefits and a sound level of technological security at reasonable costs.

Several countries, including the U.S., China and India, have legislation designed so that under specific circumstances their governmental agencies are given access to data and information stored by service providers under their jurisdiction, even if the physical storage is provided outside the territory of that country. With this in mind, a debate has arisen regarding compliance with Swedish and EU legislation when using a cloud service provided by the private market. The Swedish Social Insurance Agency notes that provisions in both Swedish and EU law prohibit Swedish governmental agencies from using certain public cloud services operated by private service providers for the purpose of handling confidential information or personal data, if said service provider is under the jurisdiction of a state that has legislation such as that described above.

We are, however, of the opinion that an essential issue has not been addressed in the Swedish debate, namely whether it is appropriate for Swedish governmental agencies to hand over to private companies or other countries control of information concerning activities which we have labelled as *sustaining societal functions.* There are also a number of security related issues. For example, the possibility of a generally greater vulnerability, an increased risk of unauthorised access to data, as well as difficulties in conducting security checks on technical staff and accurate risk and vulnerability analysis.

The Swedish Social Insurance Agency will not contract the operation of critical digital systems for sustaining societal functions to private companies under the jurisdiction of states with the type of legislation mentioned above. Regarding IT-systems in security-sensitive activities, the aim of the Swedish Social Insurance Agency is for IT-systems to be under governmental control.

In order to ensure that sustaining societal functions are secure against cyber attacks, to protect privacy and to reduce dependence on the provision of individual services by the private market, Sweden needs to formulate an overarching governmental strategy and a long-term action plan to protect digital sovereignty. In addition, in order for Swedish governmental agencies to continue to benefit from all the opportunities provided by digitalisation, we should ensure – through cooperation nationally and within the EU – that the private services we choose to use are adapted to our requirements and current legislation and have a level of security that allows us to maintain control over our functions and data. This will enable Sweden to take advantage of the innovation and efficiency benefits often associated with IT-services provided by the private market whilst at the same time securing the digital sovereignty of Sweden.

Background

The government's digital agenda for Sweden stresses the importance of private and public organisations acting in a responsible manner. Digital systems should be secure and personal privacy should be protected. The government also highlights the increased vulnerability associated with greater dependency on technology and how the general public's trust is dependent upon the security of the technology.[1]

Cloud services are becoming more commonly used, including in Swedish public agencies. In a study carried out in 2018, a large number of Sweden's public agencies indicated that they use at least one 'public cloud service' that is provided by a supplier from the private sector.[2]

1 Ministry of Enterprise and Innovation, *Med medborgaren i centrum – Regeringens strategi för en digitalt samverkande statsförvaltning [With a focus on the citizen – Government strategy for digitally collaborative state administration]* (N2012:37).

2 See Annex 2 for definitions of cloud services and a description of the use of cloud services. See Annex 1 for a historical overview of outsourcing of state administration and Hellberg, Islam, Karlsson, *Säkerhet vid molnlösningar [Security for cloud solutions]*, Örebro University and the Swedish Civil Contingencies Agency, p. 25.

Purpose

In this document we initially summarise facts that are of significance to the Swedish Social Insurance Agency's use of public cloud services offered by private suppliers. The purpose of this, first and foremost, is to provide a basis for a well-reasoned stance on the Swedish Social Insurance Agency's options for the use of these cloud services in the pursuance of our mission. We have not taken a stance on the risks associated with other supply models and technologies. Even though this white paper focuses on the activities of the Swedish Social Insurance Agency, it is our hope that the work we have carried out here might serve as a basis for other organisations who operate what we refer to as sustaining societal functions. Our hope is also that this document will lead to the question of how Sweden can ensure control over IT services in sustaining societal functions being accorded a more prominent position than it currently occupies.

The term ‘white paper' is used in various sectors and organisations, including within the EU, to express ideas and ambitions within a specific field. The term is thus well-suited to what we hope to achieve with this work. This document covers our perspective on the question of the use in the Swedish Social Insurance Agency of cloud services offered by private suppliers and it is our hope that the content might contribute to a deeper and wider discussion of a matter that is of crucial importance to society as a whole. Our conclusions, as set out in this document, will be gradually incorporated into our internal administrative management and support documents as and where relevant.

Our survey and analysis focus on the functions that we have called *sustaining societal functions*. This term is chosen because our analysis identifies a need to safeguard not only *vital societal functions* but also such functions which, although they may not count as vital societal functions themselves, are depended on by vital societal functions. By using the broader term *sustaining societal functions*, we can also expand the discussion and base it on a systematic perspective on the activities on which Sweden is dependent in order to function.

Cloud services as a supply model

Cloud services are defined as the situation where functions that would otherwise be handled by in-house computers are made available online from the service provider's computers or servers.[3] This can entail major advantages for both suppliers and clients. Previously conducted studies indicate major benefits for the public sector if this technology can be used to enable secure and cost-efficient digitalisation of operations.[4]

Cloud services are offered in three fundamental forms, based on the relationship between the client and the supplier:[5]

- *Public cloud services,* whereby a service is offered to several clients who share the same infrastructure, such as servers. The clients' data is stored separately, virtually at least.
- *Partner cloud services,* which are intended for a specific group of clients, such as public authorities. The clients' data can be stored separately, virtually at least, if this is required given the particular service.[6]
- *Private cloud services,* that the supplier only offers to a specific client.[7]

These three forms of cloud services can be provided by private or public organisations. It follows that whether the cloud service is public or private has nothing to do with who provides the service.

The challenges associated with the cloud services differ depending on how the service is designed technically and contractually. However, there is great interest in the Swedish public sector in the use of the international public cloud services offered by private companies.[8]

Against this backdrop, this white paper primarily addresses the problems that can arise when a public authority uses a public cloud service provided by private suppliers. However, some of the analysis may also be applicable to other forms of cloud services or to other forms of IT services for that matter.

3 Sometimes the terms *data cloud*, *the cloud* or *cloud services* are used.

4 Swedish Pensions Agency, *Molntjänster i staten – en ny generation av outsourcing [Cloud services in the state - a new generation of outsourcing]* 2016 and the National Government Service Centre, *En gemensam statlig molntjänst för myndigheternas it-drift* – Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner, *[A joint state cloud service for public authority IT operations – Periodic report on the government mandate on coordination and relocation of public authority activities]*, (Ref.10052- 2016/1121), 07-02-2017.

5 For a more detailed description of cloud services as a supply model, see Annex 2.

6 Some partner services are configured so that the parties involved in the collaboration can exchange and share information, whereas other partner services are configured exactly like public cloud services with entirely separate data.

7 The definitions that are used are those that have been used in the Swedish Pensions Agency Study. See the Swedish Pensions Agency, *Molntjänster i staten [Cloud Services in the State]*, p. 9. See also Annex 2.

8 See also Annex 2.

Third-country legislation on access to e-evidence – USA as an example

In order to secure access to e-evidence (i.e. digitally stored information, such as emails or details of calls, emails or text messages), some countries have enacted legislation that safeguards such evidence. The most widely discussed example of this is the US-based Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

To illustrate how such legislation can be formulated and what legal problems it can entail, we provide an overview of the CLOUD Act and the ongoing debate relating to this legislation below. In the meantime, it is important to bear in mind that similar legislation is in place in several other countries, such as China, India and Russia.[9]

The CLOUD Act – An Overview

This section provides an outline description of the CLOUD Act, which came into force in March 2018.[10] This legislation gives the American public authorities the possibility of, among other things, requiring suppliers of electronic communication services and cloud services (referred to hereinafter as service providers) under American jurisdiction, to retain or disclose data that is under said supplier's control.[11]

In this connection, it makes no difference if the information is stored or handled in or outside the USA.[12] Such a request should – to put it simply – take place via a "warrant" issued by a court, an administrative order, by subpoena of a grand jury or a court decision.[13]

9 The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Preliminary Study Report on Web-based Office Support]*, Ref. 23.2-6283-18, 22-02-2019, p. 24.

10 For a more detailed account, see, for example, Council of Bars and Law Societies of Europe, *CCBE Assessment of the U.S. CLOUD Act, 28-02-2019*. The CLOUD Act formally embodies changes and amendments to United States Code and more specifically the part that is embodied by the Stored Communication Act (SCA), which regulates the disclosure of digital communication stored by suppliers of electronic communication services, etc. (18 U.S.C. Chapter 121 2701–2712). The background to the CLOUD Act was a dispute between the United States and Microsoft, which became the subject of judicial review in the case of United States v. Microsoft Corp., 584 U.S. (2018). Microsoft had refused to disclose a private person's email messages, which were stored in Ireland, to the US Justice Department. Microsoft asserted that currently applicable legislation did not support the Justice Department's requests for access because the information was stored outside the USA. However, before the US Supreme Court ruled on the matter it became null and void as the American Congress enacted the CLOUD Act. Whether or not the requested information was subsequently disclosed under the CLOUD Act is unclear.

11 I 18 USC 2713 describes the legal entities covered by the provisions as a "provider of electronic communication service or remote computing service". It may also be noted here that the American jurisdiction is probably very expansive. According to the Electronic Frontier Foundation, the German messaging service Telegram, for example, can be considered to be subject to American jurisdiction because it provides services to American clients. See Electronic Frontier Foundation, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom*, 04-09-2018.

12 18 USC 2713

13 18 USC 2703(b)(1)(A-B)

The service provider has the possibility of disputing the authority's request for access to information in court om

- the person to whom the information relates is not a "United States Person"[14] and does not reside in the USA,
- there is a risk that the service provider would violate legislation in another country by fulfilling the request in question and
- that country has concluded an executive agreement with the USA.[15]

After such an objection, the court can rule whether these criteria are fulfilled and carry out a comity analysis, weighing the interests in favour of disclosure against those opposed to disclosure based on all the circumstances).[16] In its considerations, the court will take into account, among other things,

- the interests of the United States,
- the interests of the other country in blocking a disclosure that is prohibited according to said country's law,
- the risk from and scope of the consequences that the service provider might suffer in the event of a disclosure in violation of the law in the other country, and
- the links the service provider and the person to whom the information relates have with the USA.[17]

The extent to which a service provider can dispute a request in accordance with the CLOUD Act if the above conditions are not fulfilled is unclear.[18]

The CLOUD Act also gives the United States Attorney General the possibility, by means of an executive agreement with other states, as mentioned above, of allowing these states to request data directly from American service providers for the purpose of combatting serious crime.[19] Before such agreements are concluded, the Attorney General shall ensure, among other things, that the other country's legislation provides adequate protection for privacy and human rights, both materially and procedurally.[20]

14 A United States Person is, for example, an American citizen or someone who has the legal right to reside in the USA, see 18 USC 2703 (h) with reference to 2523 (a)(2).

15 18 USC 2703 (h) compared with 2523 (b) and (d). Note that Sweden is not currently party to any such agreement.

16 18 USC 2703 (h)(2)(B)

17 18 USC 2703 (h)(3)

18 EPDB-EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*,10-07-2019, Annex pp. 1–2.

19 Such agreements are concluded by the Attorney General after approval by the Secretary of State. The agreement must be presented to the United States Congress, which has 180 days to object to the agreement before it takes effect. See 18 USC 2523 (b) and (d).

20 18 USC 2523 (e). Such agreements are to be reviewed every five years.

The CLOUD Act debate

From a rule of law perspective, it is advantageous that the conditions for requests by United States authorities for access to data stored outside the USA are now regulated by law.[21] The major cloud service providers have also indicated their understanding that the CLOUD Act constitutes a reasonable balance between the rights of the individual and the needs of law enforcement authorities.[22] However, there is no lack of critical voices and several American technology companies have expressed misgivings that the lack of an agreement between the USA and EU with respect to law enforcement authorities' access to data puts American business interests in Europe at risk, including in relation to potential conflicts of law.[23]

Serious criticism has also been raised with respect to the protection of human rights. The Council of Bars and Law Societies of Europe argues that the CLOUD Act fails to meet the European minimum standard established by the European Court of Justice with respect to state electronic surveillance of citizens.

Several independent human rights organisations also stress that the protection of human rights is pushed aside when American enforcement authorities are given the opportunity to enter into international agreements without prior review by Congress. These organisations also assert that the CLOUD Act opens up the risk of agreements being entered into with states that are known to violate human rights. This also increases the risk that states gain access to data that is then used to violate these rights.[24]

The European Data Protection Board[25] and the European Data Protection Supervisor[26] have pointed out that the CLOUD Act also provides the possibility of requesting metadata from service providers. Moreover, these institutions stress that, under the CLOUD Act, the request does not always have to be preceded by judicial review or fulfil requirements of probable cause. Examples include administrative subpoenas and subpoenas from a grand jury.[27] If the USA enters into agreements with a third country, it also opens up the possibility for said country to monitor in real-time the communications that take place via the service providers.[28]

The European Data Protection Board and the European Data Protection Supervisor also express reservations with respect to the possibilities that the CLOUD Act gives

21 See for example 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*, White Paper, April 2019, Microsoft, *Molntjänster och säkerhet [Cloud services and security]* and Council of Bars and Law Societies of Europe, *CCBE Assessment*.

22 See for example Punke Michael, *AWS and the CLOUD Act, AWS Security Blog*, 27-05-2019.

23 ACT – The App Association et al., Open letter to Attorney General Barr, 21-06-2019.

24 Letter to the United States Congress from 24 organisations, including Amnesty International USA, the Electronic Frontier Foundation and Human Rights Watch, 12-03-2018.

25 The European Data Protection Board (EDPB) is an EU body consisting of representatives from each member state's data protection authority, and others. The EDPB's mission includes promoting the consistent application of the data protection regulation within the entire EU. Within the scope of this work, the EDPB issues guidelines for the interpretation of basic terminology in the GDPR.

26 The European Data Protection Supervisor (EDPS) monitors the processing of personal data that takes place within the EU's institutions and bodies. By giving advice, handling complaints and conducting investigations, the EDPS protects the individual's right to a private life.

27 Administrative subpoena eller grand jury subpoena.

28 EPDB-EDPS, *Joint Response*, Annex pp. 2 and 9

to American authorities to share with third countries personal data received with the legal backing of the law.[29]

A request for access to information that is stored in other states often takes place through legal instruments for mutual legal assistance, referred to as the mutual legal assistance treaty (MLAT). The procedure that is applied can be protracted, entailing major challenges with respect to fulfilling the increasing need for e-evidence in criminal investigations. With enforcement of the CLOUD Act, the MLAT procedure is not normally applied.[30]

The American Department of Justice has stated that the CLOUD Act is a step in the right direction in order to address the difficulties with respect to gaining access to crucial digital evidence that is stored in third countries.[31] However, the MLAT procedure ensures that procedural and material regulations in the country in which the information is stored are followed and that the legal authority in that country is respected.[32]

A resolution of the European Parliament stated that a more balanced solution than the CLOUD Act would be to strengthen existing international systems for mutual legal assistance for the purpose of promoting international and legal collaboration.[33] The same conclusion is reached by the Council of Bars and Law Societies of Europe which also argues that the CLOUD Act undermines the effort to adapt the international cooperation to the challenges that law enforcement authorities are encountering in the new information society.[34]

29 EPDB-EDPS, *Joint Response*, Annex pp. 2 and 9

30 U.S Department of Justice, White Paper, April 2019

31 U.S Department of Justice, White paper and Jennifer Daskal, *Unpacking the CLOUD Act, EUCRIM*, 31-01-2019

32 See Council of Bars and Law Societies of Europe, CCBE *Assessment* and Electronic Frontier Foundation, *EFF and 23 Groups Tell Congress to Oppose the CLOUD Act*, 11-03-2018. Also see the European Commission, *Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp. No. 17-2*, p. 21 and EPDB-EDPS, *Joint Response*, Annex p. 3.

33 The European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)), pp. 27 and 28

34 Council of Bars and Law Societies of Europe, *CCBE Assessment*

Conflicts between CLOUD Act type legislation, EU law and national law

As mentioned earlier, the USA is not the only state to introduce legislation empowering the country's authorities to request data and information that are stored in other states without recourse to international legal backing and without the requirement of an assessment in accordance with the legislation in the country in which the information is physically stored. Since the largest and most widely-used cloud services on the market are provided by American companies, however, it is the CLOUD Act that has been of the greatest interest in practice, at least thus far. In addition to the debate mentioned above, the discussion has addressed the conflicts between the CLOUD Act and similar legislation on the one hand and EU and national law on the other. This section provides a brief summary of the conflicts between these standards with respect to the areas of the right-of-access and secrecy and data protection.[35] An additional important, fundamental question is how the CLOUD Act and similar legislation relate to the more general protection for personal privacy that Swedish authorities are obliged to uphold in accordance with, among other things, constitutional law and international conventions.[36] This issue is not covered in this context.

Public access to information and secrecy

The principle of secrecy means that it is prohibited to reveal information, whether verbally, by disclosure of a general document or in another manner. If a piece of data is covered by a secrecy provision, then it is confidential.[37]

Before a Swedish authority makes confidential information available to a service provider, the authority must, among other things, analyse whether it entails disclosure of information in the sense set out in the Swedish Public Access to Information and Secrecy Act (2009:400). In 2018 an expert legal group from the Swedish e-collaboration programme known as eSam issued a legal statement regarding the concept of disclosing information via use of cloud services subject to foreign legislation.[38] This statement was updated in September 2019. According to eSam, the Swedish Public access to Information and Secrecy Act requires that an assessment of whether confidential information should be considered as having been disclosed when it is made accessible to a service provider shall take place in two steps.

35 For a more detailed account of these conflicts between standards, see Annex 3.

36 See Ch. 2 § 6 and the Statement of Objectives in Ch. 1 § 2 RF, Article 8 in the European Convention of 4 November 1950 on the Protection of Human Rights and Fundamental Freedoms and Articles 7 and 8 in the EU Charter of Fundamental Rights.

37 Ch. 3. § 1 Public Access to Information and Secrecy Act

38 eSam is a member-driven collaboration programme between 23 administrative agencies from the government and the Swedish Association of Local Authorities and Regions, see www.esamverka.se.

First, a check is carried out to determine whether or not the service provider is permitted according to prior agreement with the client to receive or transfer the information that is made accessible to the supplier by means of technology. This means that there should be a legally binding and authorised secrecy agreement for the supplier. Moreover, the supplier must not be bound by regulations of foreign law to disclose information without a prior secrecy review or another legal basis for disclosure under Swedish law. If these initial conditions are fulfilled, a second step is carried out in which an assessment is made to determine whether the prevailing circumstances nevertheless make it unlikely that the service provider will obtain or pass on the information.

If either of these conditions are not fulfilled, the information in question shall be considered as having been disclosed immediately after it was made accessible to the service provider.[39] If the information is confidential, the authority revealing the information must have justification by law or regulation to disclose the information.

The Legal, Financial and Administrative Service Agency agreed with eSam's assessment in 2019.[40] Moreover, the Legal, Financial and Administrative Services Agency indicated that it is inconsistent with the Swedish Public Access to Information and Secrecy Act for a service provider commissioned by a Swedish authority to disclose confidential information to a foreign authority in accordance with the CLOUD Act or similar legislation. Simply put, this is due to the fact that there is no specific legal or regulatory provision authorising such disclosure. Moreover, it is not possible to ensure that it would have been permissible to disclose information to a Swedish authority in an analogous case or to ensure that Swedish interests are respected.[41] The Legal, Financial and Administrative Services Agency also noted that a Swedish authority that allows companies subject to regulations like the CLOUD Act to handle confidential information, will be viewed as prioritising the foreign regulation over Swedish legislation.[42]

Market participants have presented an opposing view that stresses the limited number of cases relating to the disclosure of information stored outside the USA's borders in accordance with the CLOUD Act. These participants also emphasise that a more nuanced assessment must be made with respect to the term disclosure and that encryption and location of server rooms, among other things, cast the problem in a different light.[43] The Swedish Association of Local Authorities and Regions (SALAR) has, partly based on eSam's position, declared that cloud services offered by the private market - including such services with foreign ownership - are a necessary part of digitalisation. Moreover, it is SALAR's view that this development is now being hampered due to the prevailing uncertainty relating to the legal issues.

39 The eSam programme, *Rättsligt uttalande om röjande och molntjänster [Legal statement on disclosing information and cloud services]*, VER 2018:57, 23-10-2018 and the e-cooperation programme, then 20-09-2019

40 The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Web-based office support preliminary study report]*, p. 35.

41 Jfr 8 kap. 3 § OSL

42 The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Web-based office support preliminary study report]*, pp. 32–33.

43 See, among others, Microsoft, *Molntjänster och säkerhet [Cloud services and security]*, Microsoft, the Swedish Association of Local Authorities and Regions et al., Open seminar at Almedalen 2019, *CLOUD Act – obstacle or not* and Fredrik Blix and Richard Brolin, *Grönt ljus för kommuner, regioner och statliga myndigheter att överväga molntjänster [Green light for municipalities, regions and state authorities to consider cloud services]*, Cybercom Group, 04-07-2019.

SALAR has also expressed reservations with respect to the investments that have already been made by a large number of Sweden's municipalities and regions in public cloud services that are offered by the private market.[44] In regard to the term disclose, SALAR has also stated that a ruling of the Swedish Labour Court in 2019 indicated that information should not be considered in itself as having been disclosed even if it has been passed on to unauthorised parties in another country.[45]

Data protection

Transfer of personal data stored within the EU to a third country constitutes processing of personal data. The circumstances under which such processing is permitted are regulated by the European Parliament and Council Regulation (EU) 2016/679 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), referred to hereinafter as the GDPR. Before a Swedish authority discloses personal data to a service provider, the authority must analyse whether this would entail a risk that the data is processed in a manner that conflicts with the GDPR.

According to the rulings of the European Data Protection Board and the European Data Protection Supervisor, the GDPR establishes legal conditions for transfer of personal data to a third country in accordance with the CLOUD Act in exceptional cases only. These are exceptional situations in which disclosure of information is required to protect the data subject's interests. The European Data Protection Board has also stressed that when there is an international agreement on mutual legal assistance, companies within the EU should generally reject direct enquiries and refer the third-country authority to the agreement.[46]

A data controller or processor who discloses personal data to a third-country authority in violation of the GDPR runs a maximum risk of incurring a significant administrative fine. Failure to obey a request under the CLOUD Act, however, entails the risk of legal sanctions in the USA. In practice, it means that a service provider contracted by a Swedish authority runs the risk of being exposed to a conflict between EU law and American legislation.[47]

44 The Swedish Association of Local Authorities and Regions, *Ställningstagande om informationshantering i vissa molntjänster [Position on information management in certain cloud services]*, ref. no. 19/00087, 12-04-2019

45 See the Swedish Association of Local Authorities and Regions, *Molntjänster och konfidentialitetsbedömning [Cloud services and confidentiality assessment]*, p.13. The case in question is AD 2019 no. 15. The matter in the case was whether there was justification for the dismissal of the former Director General of the Swedish Transport Agency. One of the questions that was addressed was whether the state was able to corroborate that information about classified protected identities had become accessible to two storage technologies (which were unauthorised) under circumstances in which it must be assumed that they would obtain the information and that the Director General was thus guilty of negligence with respect to secret information in accordance with ch. 19 § 9 of the Swedish Penal Code.

46 EPDB-EDPS, *Joint Response*, Annex p. 3. See also the European Data Protection Board, Guidelines 2/2018 for exceptions in Article 49 in accordance under Regulation 2016/679, adopted on 25 May 2018, p. 5.

47 EPDB-EDPS, Joint Response, Annex p. 2.

A Swedish authority is probably not the data controller for the processing of personal data that takes place when an appointed data processor, such as a service provider, discloses information to a third country in breach of the agreement.[48] As a data controller, however, the public authority can only appoint processors who provide adequate guarantees that the data subject's rights are protected and that the processing takes place in accordance with the GDPR.[49] The authority that intends to utilise cloud services must therefore ensure that it does not commission a service provider who may violate the GDPR or the personal data processing agreement.

48 Refer also to Annex 3.

49 See Article 28.1 in the GDPR.

Sustaining societal functions

As mentioned earlier, we have chosen to base this white paper on what we refer to as sustaining societal functions. Following our delineations defined hereabove, some of these functions involve vital societal functions, which are what are often talked about in relation to the public authorities. Vital societal functions are defined by the provisions of the Swedish Civil Contingencies Agency (commonly referred to as MSB). A small proportion of sustaining societal functions also consists of what are known as security-sensitive activities. This term is defined in the Swedish Protective Security Act (2018:585), where special rules are established for the protection of security-sensitive data. The following section opens with an introduction to the concept of vital societal functions. From this concept, we go on to explain what we consider to be incorporated under the term sustaining societal functions. Then we outline the risks that digitalisation of sustaining societal functions entails and some of the protection that is available for data and information that are processed in sustaining societal functions.[50]

What are vital societal functions?

Total defence (the fundamental concept underpinning the Swedish defence system) consists of military and civil defence. The civil defence consists of the activities that responsible parties carry out for the purpose of enabling society to manage situations when there is a state of heightened alert. Swedish civil defence is pursued, therefore, in the activities of state authorities, municipalities, regional authorities, private companies and voluntary organisations. Sweden has three goals with respect to its civil defence, of which safeguarding the most vital societal functions is one.[51]

Vital societal functions is, according to MSB, an umbrella term comprising the activities, facilities, nodes, infrastructure and services that are of crucial importance in maintaining important societal functions within a given sector of society. These activities are carried out by a large number of private and public stakeholders.[52] Vital societal functions basically comprise such functions whose absence or deficiency may trigger crises that are a threat to society. This might also include a function that is needed to manage a potential or ongoing crisis.[53] MSB has identified eleven sectors in which vital societal functions are conducted in order to maintain important functions in society. These can be found within a broad range of sectors, including

50 Data is defined according to ISO/IEC 2382:2015 as a re-interpretable representation of information in a formalised manner suitable for communication, interpretation, or processing. Information is defined according to the same standard as knowledge concerning objects, such as facts, events, things, processes, or ideas. Information must always be considered within its context. See the International Organization for *Standardization, ISO/IEC 2382:2015(en)Information technology — Vocabulary.*

51 Bill. 2014/15:109, *Försvarspolitisk inriktning – Sveriges försvar 2016–2020 [Defence policy alignment - Sweden's defence]*, p. 12. The Swedish Armed Services Commission Report 2014/15:FöU11 and the Minutes of Parliament 2014/15:117.

52 The Swedish Civil Contingencies Agency, *Vägledning för identifiering av samhällsviktig verksamhet [Guidelines for identifying vital societal functions]*, MSB1408, June 2019, p. 7.

53 See the Swedish Civil Contingencies Agency regulations on state authorities' risk and vulnerability analyses (MSB 2016:7) § 2. Vital societal functions are defined here as activities that satisfy at least two conditions. 1) Loss or severe disruption of the function independently or in combination with equivalent events in other functions can quickly result in the emergence of a serious crisis in society. 2) The function is necessary or essential for management of a crisis in society that has already emerged so that the damaging effects are kept to the absolute minimum.

energy supply, health and medical care, welfare and transportation. Other examples are the supply of municipal technical services, including key functions such as drinking water supply, sewage management, sanitation and road maintenance, as well as social insurance, which includes the public pension system and health and unemployment insurance.[54]

What do we include in sustaining societal functions?

As indicated above, the term includes vital societal functions, which are activities essential to the functioning of our society. In order for it to work, continuity is often required in functions and IT systems that are not categorised as societally vital. For example, vital societal functions like the fire service and medical care depend on something so simple as a functioning childcare system for their staff. In this white paper, we have chosen to use the term sustaining societal functions to describe both the functions that are societally vital and those functions on which vital societal functions are in some way dependent in order to function. Our definition of sustaining societal functions is thus based on MSB's definition of vital societal functions. However, it is not easy to define the limitations for what should be considered sustaining societal functions. Society is constantly developing and the interdependencies of functions are subject to change. Therefore, it is necessary for every authority responsible for any vital societal function to identify the other functions on which this function is dependent in order to operate.

In addition to the sustaining and vital societal functions, there is a further level of functions, namely security-sensitive activities, which include functions of importance to the security of Sweden. More information about such functions is provided in the section below entitled Protective Security. The relationship between the different categories of functions can be illustrated as follows.

Illustration of the relationship between the terms sustaining societal, vital societal and security-sensitive. Some of the sustaining societal functions are comprised of vital societal functions, which, in turn consist to a certain extent of security-sensitive activities.

54 MSB, *Vägledning för identifiering av samhällsviktig verksamhet [Guidelines for identification of vital societal functions]*, p. 7.

Identified risks as a consequence of digitalisation and outsourcing of sustaining societal functions

As a consequence of, among other things, technology and service development, privatisation, outsourcing and automation, developments in society are leading to more and increasingly complex interdependencies between various functions. MSB has determined that it is important that technological development does not diminish society's ability to withstand and manage disruptions.[55]

The Swedish Security Service identified technological development as one of seven threats to Sweden in 2019.[56] The government also determined that the vulnerability in today's global IT system is one of our most complex challenges and that it will continue to be so for the foreseeable future. Activity in the cyber-environment has developed to the extent that it poses a separate threat as well as being one of many means of military force.[57] Hostile IT attacks from states or state-supported groups can be directed towards key elements of society and have a dispersing effect on vital societal functions in several sectors.[58] A permanent cross-party forum, the Swedish Defence Commission, has determined that Sweden's military defence depends on the continued operation of other basic societal functions before and during an armed attack. For this reason, it becomes all the more difficult to know where the civil infrastructure stops and the military infrastructure begins.[59] In order to maintain a high level of cyber-security in Sweden, the government has determined that it must be possible to protect vital societal functions and IT systems from IT attacks. Part of Sweden's defence policy entails that Sweden should develop and strengthen its collective capacity to prevent, counteract and actively manage the consequences of civil and military threats, events and attacks in the cyber-environment.[60]

In this context, the intelligence activity conducted by American authorities with the support of the Foreign Intelligence Surveillance Act (FISA) should be mentioned. With the PRISM system, data collected from service providers is analysed for intelligence activities relating to people other than American citizens.[61] In 2013, it was revealed that millions of user accounts, including in Google, were part of this

55 MSB, *Övergripande inriktning för samhällsskydd och beredskap [General alignment for civil protection and readiness]*, p. 7.

56 Swedish Security Service, Årsbok 2018 [2018 Annual Report], p. 21.

57 The Swedish National Defence Radio Establishment (FRA) points out that state cyber-attacks take place regularly and are increasing continually. The purpose of these attacks is indicated as being to gather information, e.g. about the strategies behind Sweden's international policy, our society's vulnerabilities or Sweden's total defence system. It can also involve preparations for subsequent attacks and disruption or industrial espionage. Refer to the Swedish National Defence Radio Establishment, 2018 Annual report, pp. 17 and 19.

58 Se Bill. 2014/15:109, p. 111–113.

59 Ds 2017:66, *Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025 [Resistance capacity - Alignment of the total defence and configuration of the civil defence 2021 - 2025]* p. 17 et seq and p. 113.

60 See Bill. 2014/15:109, p. 111–113.

61 Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 08-06-2013

monitoring and that metadata was also collected.[62] FISA is still valid, but it is unclear how it is applied and thus which data is collected with the support of the law.[63]

The Swedish Security Service has identified outsourcing of IT, which includes cloud services provided by private parties, as a potential risk. The Swedish Security Service stresses that this often involves a process in which the provider places various customers' systems and data in the same physical computer system. This entails an elevated risk, because a disruption in one customer's system can cause disruptions or failures in several other customer systems. If a large amount of confidential information is stored by a single provider, there is also a risk that they become an attractive target for intelligence gathering by other countries, and the like. The amount of information that is collected by any given provider may also mean that supplier's overall operations become of major importance for the security of Sweden.[64]

Regarding cloud services in particular, the Privacy Committee stressed that there are serious privacy risks involved with cloud services for public authorities on the whole, especially public cloud services. The reason that was given for this was, among other things, the large amount of personal data that the authorities handle, which can be sensitive from the point of view of privacy. It also has to do with the fact that public authorities are subject to a whole host of rules and regulations, for example with respect to public documents, confidentiality, archiving and protective security. According to the Privacy Committee, it is not uncommon for public authorities to purchase cloud services without discovering much about how the data is processed and disseminated within the service. Small public authorities may also lack expertise in choosing the right type of cloud service based on legal and security-related conditions. The Privacy Committee also points out that the public authorities' processing of personal data as an employer entails risks when it takes place in cloud services. The fact that the data is, to an increasing extent, stored on the premises of external providers can entail extensive dissemination, storage and further use of the data, which are difficult to keep a check on. Many elements of the processing are often carried out without the knowledge of the employer or employee.[65]

An additional risk factor deriving from outsourcing is the service provider's management of telemetry data. Telemetry data is measurement data that is collected and processed by the provider. It may comprise both actual content and metadata. In theory, such data can be subject to disclosure in accordance with legislation such as the CLOUD Act, but is processed primarily by the supplier for the purpose of improving and maintaining the service. In this context, it is interesting that a cloud service as a business model often entails an inherent motivation to use the clients data for the provider's own purposes, such as development of new services and sharing the data with other companies, for example as a basis for advertising.[66] Even if some settings can limit the amount of telemetry data that is processed by the service provider, the clients are not able to maintain complete control over the

62 Gellman Barton and Soltani Ashkan, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post, 30-10-2013

63 European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, (PE 583.137), pp.127–128

64 Swedish Security Service, *Årsbok [Annual Report]* 2017, p. 56.

65 The Privacy Committee also determined that the private individual often has no legal recourse to reject the processing of personal data by public authorities, which can have far-reaching effects with the use of cloud services, because data from the administration reaches the private sector. See the Privacy Committee, *What is the privacy situation? - A survey by the Privacy Committee* (SOU 2016:41) pp. 53–54, 70 and 81.

66 SOU 2016:41.p. 111

processing. Standard agreements for cloud services often give the provider ample opportunity to process data for their own purposes, even if such agreements violate data protection regulations. In a study conducted by Dutch authorities, it was determined that suppliers of, among other things, public cloud services collect potentially sensitive data without legal justification (including metadata) and that they disclose telemetry data to countries outside the EU.[67]

The Privacy Committee determined that the greatest risks to personal privacy with respect to cloud services are associated with the loss of transparency and control that the use of such services normally entails. In addition to the risks that have already been mentioned above, this loss also entails the risk of unauthorised parties gaining access via providers and subcontractors and the risk that the information is stored in countries where the legislation does not provide adequate protection. The data can also end up in the hands of subcontractors who are unknown to the client, which can make it difficult for a data controller to fulfil their obligation to ensure that the data is processed in accordance with data protection regulations.[68]

The Swedish Security Service has also determined that an increasing number of public authorities contract parts of their activity that are particularly in need of protection out to providers in other countries, in a process known as off-shoring.[69] In such cases, the public authorities have the same obligation to require security measures as they would if the provider were based in Sweden. MSB also determined that off-shoring requires special consideration when working with protection for vital societal functions. When outsourcing activities to a provider in another country, there should always be a bilateral protective security agreement in place between Sweden and the country in which the provider is located.[70]

In an investigation relating to the outsourcing of the Swedish Transport Agency's IT operations in 2017, it was determined that transferring control and maintenance of central parts of the technical systems that allow a Swedish public authority to actually function involved a certain level of risk. The investigators concluded that even systems that should be open and accessible and do not necessarily contain sensitive data can be so important to Swedish society that it is not appropriate to hand over control to parties located somewhere other than Sweden.[71]

67 See Annex 8 for more details on telemetry data that is processed by providers. See also SOU 2016:41 p. 112.

68 SOU 2016:41 p. 111

69 If the provider offering the cloud service stores client data or has technical personnel in another country, it is considered a form of off-shoring.

70 Swedish Security Service, *Årsbok [Annual Report]* 2017, p. 56 and the Swedish Civil Contingencies Agency (MSB), *Handlingsplan för skydd av samhällsviktig verksamhet, [Plan of action for protection of vital societal functions] MSB597, Dec. 2013*, p. 17

71 SOU 2018:6, Study of the Swedish Transport Agency's procurement of IT services, p. 238

Protection for sustaining societal functions

In this section, we give a rundown of the rules and regulations that offer protection to the activities of public authorities, with a special focus on IT support. We also cover encryption, which has been highlighted in certain contexts as a possible measure for dealing with those legal conflicts which we discussed previously, and so forth.

The identified areas should only be viewed as examples. It must be borne in mind that there are also other regulations. For example, there is legislation that protects various types of data, such as the data protection and secrecy regulation.

Risk and vulnerability analyses

Municipalities, regional authorities and the vast majority of state authorities must analyse whether there is such vulnerability or there are such threats and risks within the authority's area of responsibility that might seriously diminish the capability to function within that area (risk and vulnerability analysis).

Such an analysis is an initial step in a chain intended to identify and reduce the vulnerabilities, threats and risks within the authority's area of responsibility that might seriously diminish the capability to function within said area.[72] When the risks have been identified, the analysis is used to assess whether the risk level is acceptable and, if that is not the case, what measures might be taken to counteract the occurrence or minimise the effect of the identified risks.[73] MSB stresses that preparedness for war must also be ensured when procuring vital societal functions.[74]

Information security and information classification

All state authorities under the government must ensure that their own information management systems fulfil such basic and special security requirements that the functions of the authority can be carried out in a satisfactory way.[75] The purpose of the authorities' information security work is to maintain confidentiality, accuracy, traceability and accessibility of information. In order to achieve this, an information classification must be carried out.

This classification identifies the need for protection for a certain level of access to data. This takes place by classifying information on different levels based on the consequences that can arise as a result of deficient protection with respect to confidentiality, accuracy and accessibility.

72 Swedish Act (2006:544) on municipal and county council measures prior to and during extraordinary events in peacetime and during periods of heightened alert ch. 2 §|1 and Ordinance (2015:1052) on emergency preparedness and surveillance responsible authorities' measures at heightened alert § 8 and § 16 2

73 The Swedish Civil Contingencies Agency (MSB), *Vägledning för risk- och sårbarhetsanalyser, [Guidelines for risk and vulnerability analyses],* MSB245, April 2011, pp. 50–51

74 The Swedish Civil Contingencies Agency, *Upphandling till samhällsviktig verksamhet – en vägledning [Procurement for vital societal functions - guidelines]*, MSB1275, September 2018, p. 19

75 See §§ 3 and 19 of Ordinance (2015:1052) on emergency preparedness and surveillance responsible authorities' measures at heightened alert

Based on the results of the information classification and risk analysis, the public authority must then identify and implement the measures that are required to fulfil the protection need. Each individual public authority must decide which model should be applied for their work.[76]

Protective Security

As mentioned earlier, part of what we call sustaining societal functions consists of what are known as security-sensitive activities, which includes functions that are important to the security of Sweden. The Swedish Security Act regulates how such functions should be protected against espionage, sabotage, terrorism and other threats in a preventative manner.[77]

Security-sensitive activities are classified based on the damage that Sweden's security might incur if an attacker should collect information about such functions, destroy data or prevent the function from being carried out in another manner.[78] The requirements on processing protective security classified information become more stringent in line with the level of classification. Security-sensitive activities are conducted by, among others, Swedish public authorities, such as the Swedish Social Insurance Agency.

The Swedish Protective Security Act includes provisions on data and personnel security. Data security involves protecting data, regardless of where it is located, in a manner such that it cannot be disclosed or changed by unauthorised persons. It also involves ensuring that data is accessible when it is needed.[79]

Personnel security means that a job title or other position involved in a security-sensitive activity is normally assigned a security class on the basis of the type of data to which the person can gain access and the extent to which this may take place.[80] The party that employs or contracts a person in security-sensitive functions must first conduct a security check, which demonstrates whether the person can be considered loyal to the interests that should be protected and is otherwise trustworthy from a security perspective.[81] The security check includes a basic assessment that may involve an interview and the collection of relevant certificates and references.[82] The basic assessment is followed by a check of official registers carried out by the Swedish Security Service.[83] This comprises information that is collected from criminal records, the Swedish police "suspicion directory" and information that is processed under the Swedish Act (2018:1693) on processing of personal data by the

76 §§ 4 and 9 of the Swedish Civil Contingencies Agency's provisions for governmental authorities' information security (MSBFS 2016:1)

77 ch. 1 §§ 1–2 Swedish Protective Security Act

78 ch. 2 §5 Swedish Protective Security Act. The four security classifications are 1) classified (top secret) if the damage that can occur is exceptionally grave, 2) secret causing serious damage, 3) confidential causing damage that is not insignificant and 4) restricted secrecy causing only minor damage.

79 ch. 2 § 2 Swedish Protective Security Act. See also the Swedish Security Service, *Informationssäkerhet [Data security]*.

80 ch. 3 §§ 5–10 Swedish Protective Security Act

81 ch. 2 § 4 and ch. 3 §§ 1–2 Swedish Protective Security Act. See also the Swedish Security Service, *Personalsäkerhet [Personnel security]*.

82 ch. 3 §§ 3 and 4 Swedish Protective Security Act (2018:585), ch. 5 § 2 Swedish Protective Security Ordinance (2018:658) and ch. 6 § 4 the Swedish Security Service's regulations (PMFS 2019:2) on protective security See also the Swedish Security Service, *Vägledning i säkerhetsskydd [Guidelines for protective security]*, pp1. 1–12

83 ch. 3 § 14 Swedish Protective Security Act (2018:585)

police within the Swedish Criminal Data Act.[84] Swedish citizenship is not a requirement for people to participate in security-sensitive activities conducted by state, municipality or regional authority in a manner other than through employment.[85] If the person who is to be employed or contracted resides or has resided in another country, the Swedish Security Service's options for conducting qualitative register checks are limited, however. The Swedish Security Service has determined that the party carrying out the activity must be prepared for this by means of greater scrutiny in background checks and being more stringent in the collection of references and suchlike..[86] One example of the difficulties related to background checks of foreign citizens was illustrated in the investigation conducted in 2018 with respect to the Swedish Transport Agency's procurement of IT services.[87]

If a public authority's security-sensitive activity is operated by a tendering service provider, the authority must require the same level of security protection that would be required within its own internal activities.[88] This takes place with a protective security agreement concluded by the tendering party, the provider and any subcontractors. The authority must also check and follow up to ensure that the providers have actually taken the measures that the authority requires by means of the protective security agreement.[89] One of the risks involved with procurement in connection with security-sensitive activities is, according to the Swedish Security Service, that the requirements specified in the protective security agreement are sometimes defined so generally that they are difficult to monitor.[90]

84 ch. 3 § 13 Swedish Protective Security Act

85 ch. 3 11 § Swedish Protective Security Act

86 Swedish Security Service, *Vägledning i säkerhetsskydd [Guidelines for protective security]*, p. 26.

87 See SOU 2018:6, pp.161–163.

88 The Swedish Security Service, Protective security for public procurement and commercial agreements.

89 ch. 2 § 6 Swedish Protective Security Act. The decision relates to procurements and agreements relating to goods or construction contracts if there is information in the subject of procurement that is security classified as confidential or higher, or if the procurement otherwise relates to or gives the provider access to a security-sensitive activity of importance to the security of Sweden.

90 Swedish Security Service, *Årsbok [Annual Report]* 2017, p. 56.

Encryption of Data

All people carrying out work - public and private - must protect information with the aid of encryption functions that have been approved by the Swedish Armed Forces when security classified information is communicated to an information system outside that person's control.[91] Many cloud service providers also offer their clients encryption services for functions and activities that do not fall under the Protective Security Ordinance. In some contexts, it has been suggested that problems related to third-country authorities' access to data stored in cloud services can be mitigated with the aid of such services.[92]

The purpose of encryption is clearly to prevent unauthorised parties from gaining access to data. If the service is designed so that a party, such as the service provider, can be considered authorised and thus gain access to the encryption key, the encryption does not protect against said party's access. Encryption normally has a negative influence on performance if the access to data is limited for the provider. Encrypted data cannot be processed either, which means that potential areas of application for many services are seriously limited.[93] The Legal, Financial and Administrative Services Agency concluded in their preliminary study relating to web-based office support that encryption is not a realistic protective measure for office applications.[94]

91 ch. 3, § 5 Swedish Protective Security Ordinance (2018:658)

92 For further information on encryption refer to Annex 7.

93 In practice, processing refers to all measures taken so that data can be handled in manner other than storage or transmission. If the information is to be read or deleted, this is referred to as processing. Encrypted data can be likened to a letter in a closed envelope, where the envelope represents the encryption. This envelope can be stored and moved, but the envelope must be opened in order to access the contents, which is equivalent to decrypting data. Refer also to Annex 7.

94 The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Web-based office support preliminary study report]*, p. 35. In the analysis of Microsoft's use of telemetry data that Dutch authorities conducted in 2017, encryption was not mentioned as a way to address the problem of the service provider having access to sensitive data from their customers. Refer also to Annex 8.

Digital Sovereignty

The ultimate purpose of Sweden's security policy is to guarantee the country's autonomy and independence. It is a matter of protecting our sovereignty, Swedish rights and interests and our fundamental values, as well as protecting Swedish freedom from political, military or other pressure. The government has now declared that a necessary condition for Sweden to achieve the goals for our security is that we assert our country's sovereignty and territorial integrity.[95]

National sovereignty is defined as control over a nation's territory, national control over the political decision-making processes in the country and securing of the nation's supply of basic necessities. National sovereignty can be considered a prerequisite for the ability to protect other values, such as human lives and health, the functioning of society as well as democracy and the rule of law.[96]

At a time when sustaining societal functions are increasingly dependent on digital systems, control of information in such functions becomes even more important for our country's independence. The Swedish Defence Commission stresses that advanced capability in the information and cybersecurity field increases the possibility of maintaining our national sovereignty, actively contributing to management of local conflicts and protecting critical infrastructure.[97]

The term digital sovereignty was used for the first time in the early 2000s. France seems to be one place where the concept was originally discussed.[98] However, discussions did not truly get going until 2013 in connection with the revelation that some countries had been conducting massive digital surveillance of European, as well as other, citizens.[99] Among the measures that were discussed at the time were a national notification service (Germany), dedicated underwater cables for internet traffic (Finland and EU), local cloud services for storage (France, Germany, Switzerland and Poland) and networks to protect data traffic from leaving the EU (Germany).[100]

France and Germany announced in 2015 that they will jointly pursue the matter of digital sovereignty at the EU level. This meant enhancing the Member States' and EU's capacity to protect digital networks, to develop an autonomous, innovative, effective and diversified digital industry, particularly with respect to cybersecurity and related services in Europe and that Europe should be able to independently

95 Government bill. 2014/15:109 p. 7

96 See MSB,MSB, *Övergripande inriktning för samhällsskydd och beredskap [General alignment for civil protection and readiness]*, p. 7–8.

97 Ds 2017:66, p. 115

98 Bellanger Pierre, De la souveraineté en général et de la souveraineté numérique en particulier, Les Échos, 30/08/2011. Initially the term technological sovereignty was also used, see Maurer Tim, et al., *Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013*, New America's Open Technology Institute and the Global Public Policy Institute (GPPi), p. 4.

99 Tim Maurer et al., *Technological Sovereignty*, p. 3. Supervision was regulated in the American executive order 12333: Office of the Director of National Intelligence *United States Intelligence Activities (Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008)).*

100 Tim Maurer et al., *Technological Sovereignty*, p. 11.

determine the security level for its own data.[101] Digital sovereignty on the EU level has also been mentioned on other occasions. The European Council reasons that it needs to be ensured that Europe has digital sovereignty and gains its fair share of the benefits associated with the digital transformation.[102]

Conclusions by the Council of the European Union regarding the future with a heavily digitalised Europe post 2020 underscore how Europe's capacity for cybersecurity must be enhanced in order to protect Europe's digital sovereignty.[103] The question of the sovereignty of EU countries in important technological areas has also been identified by the EU Commission's acting President Ursula von der Leyen as one of the measures to equip Europe for the digital age.[104] Representatives of the European Data Protection Supervisor have also touched on the issue of digital sovereignty by stating that a requirement for maintained sovereignty is that authorities protect the entire critical supply chain and ensure that 'exit strategies' are in place when they use cloud services.[105]

Nevertheless, the meaning of the term digital sovereignty has not been clarified. The German Digital Summit's recommendations for how Germany should maintain digital sovereignty proposed the following definition.[106]

A state or organisation's digital sovereignty includes complete control over stored and processed data, as well as independent decision-making about who gains access to data. This also includes the ability to independently develop technical components and systems and to change, manage and complement these components and systems with other functions.[107]

The German Ministry of the Interior indicated in September 2019 that the Ministry will work in the coming years to strengthen the public administration's digital sovereignty. This will take place by means of decreasing dependency on individual IT providers. Alternative programmes are also being taken into consideration in order to replace certain software from these suppliers after reconciliation at the EU

101 This was announced in a joint declaration in connection with a ministerial meeting in 2016. See Le ministère de l'Europe et des Affaires étrangères, *Déclaration du conseil franco-allemand de sécurité et de défense,* 2015.

102 The European Council, A New Strategic Agenda for 2019–2024, June 2019.

103 The European Union Council (Transport, Telecommunications and Energy Council), Conclusions on the Future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion", 2019-06-07, p. 5, conclusion 7.

104 von der Leyen Ursula, Political Guidelines for the Next European Commission, 2019–2024, p. 5

105 Robert Riemann at EDPS, cited at the first European Software and Cloud Suppliers Customers Council, 29/08/2019. See Huizing Lennart, *The Hague Forum for Cloud Contracting*, Privacy Company, 24-10-2019. An exit strategy is an agreement that describes the economic and technical conditions for replacement of providers and moving data when necessary.

106 The Digital Summit (Digital Gipfel) is a collaboration between politics, the commercial sector, research and society that is administered by the German Federal Ministry of Economic Affairs and Energy (Bundesministerium für Wirtschaft und Energie). The collaboration is implemented through various platforms, of which 'Innovative Digitalisation of the Economy' (Innovative Digitalisierung der Wirtschaft) is one. Project work is done in focus groups within the platform. The 'Digital Sovereignty' focus group presented its recommendations for action with respect to digital sovereignty in 2018 with a special focus on artificial intelligence. For further information, refer to the German Federal Ministry of Economic Affairs and Energy, *Digital Summit.*

107 See Digital Gipfel, *Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen [Digital Summit - Digital Sovereignty and Artificial Intelligence - Conditions, Responsibilities and Recommended Actions]*, 2018, p. 3

level.[108] The proposal was solidified in October 2019 with Project GAIA-X, which is described as a federated data infrastructure. The purpose indicated is to secure digital sovereignty, reduce dependence and enable innovation and use of cloud services that do not conflict with European law.[109]

In order to enable the use of private service providers, the Federal Department of Economic Affairs and Energy in Germany also published criteria that cloud services must fulfil in order to receive the 'trusted cloud service' quality stamp. Requirements are specified for the provider's profile, possibilities of auditing, how agreements can be signed, subcontractors, security, privacy, operative processes, interoperability, architecture and services.[110] The services that fulfil the criteria are made public after they have been certified.[111]

A government bill was recently adopted in Sweden with a proposal for changes to the Swedish law on electronic communication and the Public Access To Information And Secrecy Act in order to be able to protect Sweden's security during the use of radio transmitters. The government's rationale for the bill was similar to that which was submitted by the German Digital Summit. The term digital sovereignty is not mentioned expressly, though. The government emphasised, however, that when the protection for vital societal infrastructure is designed, consideration must be given to how security and accessibility may be affected by the access to and control of components, systems and infrastructure that private or foreign ownership and outsourcing involve. It has also been reasoned that an attack on vital societal systems by state or state-supported parties constitutes a serious threat to societal functions and the assertion of our sovereignty and territorial integrity.[112]

108 The Federal Ministry of the Interior, Building and Community, *BMI intensifies activities to strengthen digital sovereignty in public administration*, 19-09-2019

109 Federal Ministry for Economic Affairs and Energy (BMWi), *Project GAIA-X A Federated Data Infrastructure as the cradle of a vibrant European ecosystem,* p. 6–9, 12

110 Federal Ministry for Economic Affairs and Energy (BMWi) *Criteria and catalogue for cloud services version 2*

111 Federal Ministry for Economic Affairs and Energy (BMWi), *Trusted Cloud – Cloud providers*

112 Bill. 2019/20:15, *Protection of Sweden's security when radio transmitters are used* , p. 26

Conclusions of the Swedish Social Insurance Agency

There are conflicts between possibilities for third-country authorities to request data that is stored by service providers under their jurisdiction and EU law and Swedish provisions with respect to data protection and secrecy.

However, the starting point for the discussion about the IT environment of sustaining societal functions should not be these conflicts between standards, but the issues of principle that arise when control over the function's data is transferred to private companies or foreign authorities.

Digital systems that are critical to activities in the Swedish Social Insurance Agency's sustaining societal functions should be under the control of the Swedish state administration.

The Swedish Social Insurance Agency will not transfer the operation of digital systems that are critical to the execution of sustaining societal functions to private companies that are under the jurisdiction of a state that has legislation of the CLOUD Act type. For IT systems in certain functions, such as security-sensitive functions, the Swedish Social Insurance Agency's goal for the future is for our IT service to be under state management

In order to safeguard sustaining societal functions from attacks and to reduce dependency on individual private companies, Sweden's digital strategy should be complemented by the adoption of a stance on the meaning and value of digital sovereignty.

To the extent that privately operated public cloud services are used by Swedish authorities, the authorities must determine the terms and conditions for the service provision. By means of collaboration both nationally and at the EU level, Sweden's public organisations should ensure that the services that we wish to use are provided in accordance with terms and conditions that comply with Swedish legislation and ensure an adequate level of security.

Public cloud services have major advantages

In our opinion, the public cloud services that are available on the market offer many advantages. The transition to such cloud services has, in many cases, led to increased activity utilisation, increased technological security and accessibility at reasonable costs.[113] Therefore, it is desirable and often necessary for public authorities to use such technology and take advantage of the innovative capability in the private sector. Nevertheless, these positive effects should not mean that Swedish public authorities use public cloud services without first assessing the consequences from a societal perspective and for the personal privacy of individuals**.** The following section includes an assessment specifically for the Swedish Social Insurance Agency.

113 See the Privacy Committee, *What is the privacy situation? - A survey by the Privacy Committee* (SOU 2016:41) p. 110. The Committee has determined, however, that cloud services also entail major risks for public authorities.

The conflicts regarding standards with use of cloud services under private management have been identified

With respect to the CLOUD Act and similar legislation, the debate in Sweden has largely revolved around the conflicts that arise between the rights of authorities in third countries to request data that is stored by service providers under their jurisdiction on the one hand and EU law and Swedish provisions relating to data protection and confidentiality on the other. With respect to data protection, we can conclude that the European Data Protection Board stated that only in exceptional cases is the transfer of personal data in accordance with legislation like the CLOUD Act consistent with the GDPR. In view of the Board's composition and mission, these statements have a major bearing while an ultimate ruling by the European Court of Justice is awaited to settle the matter or until the legal situation changes.[114]

After the analysis carried out in the compiling of this white paper, we do not make any assessment differing from that of eSam and the Legal, Financial and Administrative Services Agency on the relationship to the Swedish Public Access to Information and Secrecy Act's concept of 'disclosure' of information. Contracting service providers who are able to release data to another country's authorities cannot be considered consistent with the basic principles in the Swedish Public Access to Information and Secrecy Act, which stipulates that it is *the Swedish public authority* (not the service provider or a foreign authority) who should make an assessment of such release *in each individual case*.[115]

The fact that all confidential information made accessible to a service provider subject to the CLOUD Act or similar legislation must be considered as disclosed means that the conflict between standards cannot be resolved by means of risk analyses. Regarding confidential data, a risk analysis would only help in an assessment of which of the data the authority is prepared to disclose in order to take advantage of the cloud service. We consider this an unacceptable position. All confidential information must be protected against unlawful disclosure and a review of a request for disclosure must take place in each individual case, not by means of an overall risk analysis.

Encryption cannot resolve the conflicts between standards even if it offers comprehensive protection against unauthorised access by hostile parties. Firstly, it cannot be ruled out that a public authority in another country that considers itself authorised to access data also considers itself authorised to access the encryption keys. It is not currently possible to determine the outcome of such a dispute. Secondly, the encryption methods that would hamper such access would greatly diminish a large portion of the service functionality.

114 Note that an agreement between the EU and USA could place the European Data Protection Board's position in a different light.

115 This is a regulation that will probably remain in place. The conditions for the study that will investigate secure and cost-effective IT operation for the public administration include that potential changes in the Swedish Public Access to Information and Secrecy Act should not entail a change or supplement to the law's provisions on decision-making procedure or the methodology of the confidentiality review. See dir 2019:64.

The conflicts between standards are only part of the problem

Much of the Swedish debate is preoccupied with attempting to estimate the extent to which Swedish authorities' data in public cloud services could be transferred to third countries in accordance with the CLOUD Act or similar legislation. We have found that the discussion this last year about the use of public cloud services offered by private companies has suffered an unfortunate bias against the already settled question of what the data protection and secrecy regulation permits. This has had the effect of other more urgent questions being overshadowed.

We have determined that it is high time to bring the discussion to a more principled level. We in the public sector must ask ourselves (and answer) how we view the *possibility* of other countries, unilaterally in accordance with their legislation, accessing data belonging to Swedish public authorities. How such possibilities are currently exercised is inconsequential. We must also shift focus from the current conflicts between standards and consider the possibility for other countries to gain access to Swedish public authorities' data from the perspective of appropriateness. There are a number of questions that need to be posed and answered. Up to this point we have identified four:

Is it appropriate for Swedish public authorities to entrust sustaining societal functions to service providers who are under the jurisdiction of another state with the possibility of said state gaining access to information about those functions without Swedish consent?

Is it appropriate for Swedish public authorities to allow a commercial party make the decision about contesting a request for transfer of confidential information to other countries' public authorities?

Is it appropriate for Swedish public authorities not to have complete control and decision-making rights with respect to which other countries can receive information from within our sustaining societal functions after agreement with the public authorities in the service provider's 'home country'?

Is it appropriate that Sweden, as a consequence of access to data in cloud services, essentially transfers legislative authority with respect to the processing of Swedish authorities' data to another country?

In our opinion, these questions must be considered in the general appropriateness assessment that should be carried out before an authority decides to use the public cloud services offered by providers on the market. These questions also direct thinking to another, more urgent discussion – that of our collective responsibility to ensure protection of activities that are important in order for Swedish society to function.

Use of public cloud services under private management increases vulnerability and privacy risks

The focus in this white paper is on the use of public cloud services under private management. With respect to public outsourcing, there is a whole host of problems related to the protection of the functions of Swedish society and personal privacy and we have identified the following as being the most significant.

General vulnerability increases

As we outlined earlier, the use of public cloud services under private management, just like other types of outsourcing, entails the risk that hostile IT attacks from state or state-supported parties can become more complex. It is also important to take into consideration the risk that a large amount of data from Swedish authorities may be collected by a single service provider, because a small number of service providers dominate the market. This increases vulnerability, because disruption to a service might affect a number of authorities at the same time. When large amounts of data are collected in the same location, this also increases the risk of attack for the purpose of intelligence-gathering.[116] The individual authorities lack information about individual service providers' cumulated access to Swedish data. If the Swedish public sector thus lacks an overall perspective, there is no overview of the cumulated dependency on various service providers, which further exacerbates the overall risks for society.

These risks arise regardless of whether the services are offered as cloud services or not. Since cloud services can normally be offered to a larger number of customers in the same physical infrastructure, these risks are greater with cloud services than with other supply models.[117]

The risk of unauthorised parties gaining access to data increases

The CLOUD Act and similar legislation have helped shed light on the debate surrounding Swedish public authorities' control over their own data. Nevertheless, such legislation is not the only reason for caution with respect to the use of cloud services under private management. This is illustrated not least by the revelations in 2013 about the American authorities' surveillance of European and other citizens. Even more important to consider is the intelligence activities that are systematically conducted by Russia, China and Iran and others, which require that Swedish public authorities carry out systematic cybersecurity work.[118] Against the backdrop of the current security situation and increasingly improving technological capabilities, the risk that foreign authorities access data belonging to Swedish sustaining societal functions or information that is confidential or protected by GDPR must be taken more seriously than was hitherto the case.

In addition to this, service providers will obtain telemetry data from clients from the software that they provide, citing the necessity to maintain and improve the service. This is important to bear in mind, not least for public cloud services, where the provider has greater access to data. The analysis that was commissioned by the Dutch authorities indicates that the service providers collected data in violation of the GDPR without indicating that they would do so in the contracts and without explicit consent of the users.[119] This is deeply troubling and affects trust in the ability of the service providers to meet the requirements on protection of information that should be in place. Even if the telemetry data collected were only to be used by the service provider for the purpose of improving the service's functionality, it is damaging that

116 The risks associated with a concentration of data must, of course, also be taken into account when internal technical solutions or solutions between public authorities are developed.

117 It should be noted that the risks from a concentration of data and functions apply whether the service provider is public or private.

118 See Kristiansson Stefan, *Om underrättelsehotet mot Sverige, [The intelligence threat against Sweden*], Frivärld, Report no. 7 2019.

119 Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data*, see also Annex 8.

the clients do not have transparency in the process nor the possibility to check which data is collected or the possibility to object to or limit the collection of such data. Moreover, it is extremely serious that data about Sweden's sustaining societal functions and personal data, including sensitive information, can become accessible to unauthorised parties in this manner. When suppliers handle personal data in a manner that is not indicated in the terms and conditions of use and the data is made accessible to third parties, the example with Cambridge Analytica shows that access to large amounts of data can have an impact on a democratic state's most fundamental interests.[120]

Background checks on personnel and monitoring become impossible or are impeded

When a Swedish public authority that conducts a security-sensitive activity uses IT services where technical personnel are not located in Sweden, difficulties arise in connection with background checks. The suppliers of global public cloud services normally have technical personnel in a large number of countries in order to ensure a high level of availability. The technical personnel are seldom selected beforehand to work for a specific client and, at the same time, the background check must be done on an individual basis. Even if the service provider were to use named personnel for their service, register checks, which are an important part of the background check, are not as effective a tool with respect to people residing in countries other than Sweden. Therefore, this must be compensated for by expanding the other components of the background check. However, it is important to reflect on the public authorities' possibilities of following up on concluded security protection agreements in practice when a public, global cloud service is used and personnel and data are scattered around the world.

Risk assessments are impeded

Ultimately, when it comes to the Cloud Act, there are still numerous uncertainties, including how legislative acts will be applied in relation to Swedish authorities' data and the extent to which such data will be requested. Then there are uncertainties with respect to the weighing of American interests against Swedish interests that the American court will have to carry out after a service provider disputes a request for submission of information. Moreover, which countries American authorities will enter into agreements with on gathering of information using the support of the Cloud Act and to what extent is uncertain.[121]

Against this backdrop, the Swedish Social Insurance Agency has determined that it is not currently possible to gain an overview of the consequences for a Swedish public authority that uses cloud services when the provider is under American

120 Cambridge Analytica was a company that offered political consulting services combined with data analysis and strategic communication. The company entered into bankruptcy after it was revealed that they used the Facebook platform to identify and influence potential voters in violation of the terms and conditions of use. The company's activities were assessed as having influenced the outcome of elections in the USA, the United Kingdom, the Philippines, and elsewhere. Further reading: Auchard Eric, *Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV, Reuters,* 20-03-2018, Cadwalladr, Carole, *The Great British Brexit robbery how our democracy was hijacked, The Guardian,* 07-05-2017 and Gutierrez Natashya, *Did Cambridge Analytica use Filipinos' Facebook data to help Duterte win?* Rappler, 05-04-2018.

121 However, it may be noted that an initial agreement that was concluded with the United Kingdom in October 2019, will be presented to the United States Congress. See Department of Justice, Office of Public Affairs, *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online,* 03-10-2019.

jurisdiction, as is the case with many of the commercial providers. This, in turn, means that it becomes difficult to implement consequence assessments in accordance with GDPR and risk and vulnerability analyses prior to procurement of cloud services, which is an equitable way of mitigating the risks involved with transferring elements of the functions to a private service provider. The CLOUD Act has served as an example, but the problems exist for all cloud services offered by a service provider in a third country with legislation that gives the country's authorities access to data that is stored by service providers under their jurisdiction. Since services can consist of a number of underlying services from different providers that may be subject to changes in ownership, the future risks become difficult to estimate. This applies in particular when the legislation in the supplier's 'home country' changes. It is also possible that a supplier's 'home country' enters into an agreement with a third country that has legislation similar to the CLOUD Act.

Privacy-related risks

Factors that increase the vulnerability of public authorities simultaneously entail an increased risk for personal privacy. For example, there are risks of unauthorised parties gaining access to data, that it is not possible to gain an overview of all subcontractors and that the data may be used for purposes other than those agreed upon. As the Privacy Committee concluded, authorities often handle a large amount of personal data. This often belongs to the category of sensitive personal data, or is privacy-sensitive in another way. In our view, this also entails that the loss of control over the information and the lack of transparency regarding how the information is handled in a cloud service constitutes an especially great risk from a privacy perspective, for public authorities in particular.

The Swedish Social Insurance Agency's position on future use of public cloud services under private management

As indicated above, there are currently numerous, serious security-related problems associated with Swedish public authorities' use of many market-leading public cloud services under private management. Many cloud services certainly involve a higher security level from a technological perspective and higher accessibility. However, this does not outweigh the fact that the use of these services means that Swedish public authorities lose control over data. An obvious fundamental basis for the public authorities' digitalisation should, in our opinion, be that we do not accept a lower level of protection for the information that is handled in the cloud service than the information that is handled in the public authorities' internal systems. In addition, there is the question of appropriateness.

When the Swedish Social Insurance Agency carries out an overall assessment of the security aspects and the questions relating to appropriateness that are identified in this work, we have determined - regardless of the existence of conflicts between standards - that systems that are critical to digital functions within our sustaining societal functions should remain under the control of the Swedish state administration. In practice, this stance means, among other things, that the Swedish Social Insurance Agency will not transfer operation of such systems to private companies that are under the jurisdiction of a country having legislation similar to the CLOUD Act. This position will, of course, have to be reviewed if proposals from the recently established state investigation of secure and cost-effective state IT-operation for the public administration are adopted and put our position in a different light.

The position does not mean that state stewardship is the only solution. For certain types of sustaining societal systems, cloud systems under private management can, under the prevailing circumstances, be procured from private companies in Sweden or within the EU in certain cases, if doing so is consistent with public procurement regulations. Whether that can happen and whether it is appropriate to use service providers outside Sweden must be determined in each individual case based on the type of function and how sensitive the data handled in the system is for Sweden's security and for private individuals. One requirement is, of course, that the terms of agreement also enable an adequate level of security and control over the data to ensure that it is not transferred to a third country. To the extent that private services are used, they must obviously also fulfil requirements in the applicable legislation.

In our opinion, certain sustaining societal functions require stricter state control and management. For the Swedish Social Insurance Agency, this involves security-sensitive activities. For IT systems in such activities, the Swedish Social Insurance Agency's goal for the future will be to keep our IT operation under state management.

In order to ensure that an adequate level of digital data protection is maintained for each individual decision in each individual authority, it is also necessary, according to the Swedish Social Insurance Agency, that Sweden as a nation will begin a more comprehensive discussion about digital protection values.

Digital sovereignty – a path to reduced vulnerability

Introduction

An increasing proportion of Sweden's sustaining societal functions are dependent on the continuity of various IT systems. There is, therefore, every reason to take the risks identified by the Swedish Security Service very seriously with respect to the technical development and outsourcing of IT. Protection of the public authorities' IT systems is also a part of Sweden's defence policy, because the lines between civil and military infrastructure become blurred in a society that is becoming all the more dependent on technology.

As is clear from Sweden's digital strategy, Swedish public authorities must assume responsibility for ensuring that digital systems are secure and that personal privacy is defended. We can only conclude that this cannot be carried out without insight into the vulnerability our dependency on various IT systems entails and the inter-dependence between various types of functions in society, regardless of whether they are categorised as vital societal functions or not. In our judgement, for this issue to gain the attention that it deserves, it is crucial that the part of sovereignty related to control over activities in IT environments is made much more clearly visible than hitherto.

Sweden's digital sovereignty must be moved up on the agenda

As MSB concluded, the term national sovereignty points towards the state's ability to secure control over its territory, political decision-making processes and supply of basic necessities. If Sweden cannot secure its sovereignty, we cannot secure societal functions or ensure protection for democracy or rule of law.

In an increasingly digital world, the control over information in sustaining societal functions is all the more important for our country's ability to remain independent. Against this backdrop, we consider it high time for Sweden to broaden its view on what sovereignty actually signifies. In the same manner that Sweden needs to

maintain its sovereignty in a more traditional sense, we must also clarify how its digital sovereignty should be maintained.

An initial step on this path has been taken by the government by means of the decision to give the Swedish National Defence Radio Establishment, the Swedish Armed Forces, the Swedish Civil Contingencies Agency and the Swedish Security Service the task of making preparations for the creation of a national cybersecurity centre.[122] As the Swedish Defence Commission concluded, advanced capability in the information and cybersecurity area would increase the possibilities of maintaining sovereignty.

In order to maintain digital sovereignty, we in Sweden must also identify what we think should fall under the concept on an overall level. The discussions conducted within the EU and by its Member States - and which the government has touched on with the Bill on the protection of Sweden's security when radio transmitters are used - have dealt with self-determination and complete control with respect to how the public authorities' IT systems should be designed and used. They have also dealt control over data that is stored in these systems and who provides access to the systems. We believe that this can serve as a starting point for defining how we should approach the concept here in Sweden. It is ultimately a matter of securing our sustaining societal functions against attacks from other states and minimising dependency on individual services on the market. The purpose of this is to protect our society and the rights of our citizens.

Just as with other aspects of sovereignty, there will always be different types of dependency, in terms of other states and private parties alike. It is not certain that digital sovereignty requires complete independence from private or foreign parties. Nevertheless, based on the changing world that we are experiencing and the vulnerability that dependency on digital systems entails for us as a nation, we must ask ourselves the following question.

How much control is reasonable for Swedish public authorities to maintain over sustaining societal functions in the IT environment?

In answering the question, we must first take into account the fact that the more we relinquish control the greater the risk of hostile attacks. Another important aspect is that we must, for each individual decision, take into account the country's collective dependency on any given service provider or any given service and the risks and confining impact of such dependency. Several factors that are currently uncertain must also be included in the assessment. For example, in the current security policy situation, we cannot rule out the risk that Sweden might be drawn into conflicts between other countries as a third party and that this would affect our digital vulnerability. We must also take into consideration the matter of trust. If Swedish public authorities prioritise gains in efficiency and short-term financial gains over protection for societal functions or personal privacy of individuals, in the long term we risk losing the trust of the general public in the public administration.

[122] Swedish Ministry of Defence, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter [Commission to establish a national cybersecurity centre]* Fö2019/01000/SUND, 26-09-2019

In order to secure Sweden's digital sovereignty, clear governance and a long-term plan of action are needed

Regardless of the meaning we ultimately assign to the concept of digital sovereignty, it is essential that the issue be addressed on an overall level spanning across public authorities and that the Swedish public administration is considered as a whole. Currently, Sweden's collective strategy for protection of our sustaining societal functions in IT environments consists, in practice, of the sum of individual authorities' considered and unconsidered decisions. The Swedish Social Insurance Agency views this as an overly passive approach to a question that is crucial to how the state administration can take advantage of the possibilities of digitalisation and to how sustaining societal digital systems may be protected. We now have the opportunity to follow Germany's and the Netherlands' good initiative to strengthen the public administration's control over data and decrease dependency on individual IT providers. In this manner we can reverse the current trend, where control over society's functions is at risk of being transferred to foreign companies and other states.

We are firmly convinced that the state administration can continue to benefit from all of the advantages of digitalisation and at the same time maintain its independence. We have strong faith in what private and public innovators can achieve in a relatively short time on the condition that there are adequate resources available and a clear direction for the work. This can, however, only be achieved after a careful analysis based on facts and decisions made centrally at an adequately high level.

Now is the time for active decisions on how Sweden's digital sovereignty should be defined and secured. Clear state governance and a sustainable long-term plan of action are needed for the protection of the IT systems that are part of our sustaining societal functions. Therefore, it is our assessment that Sweden's digital should be complemented with a clearer stance on digital sovereignty. Only when such governance is in place can Swedish authorities assume the full responsibility that is required to secure these functions in practice.

Access to physical infrastructure must be expanded quickly

In order to enable secure IT services for Swedish public authorities in practice, the physical conditions must be secured. No entity is currently tasked with ensuring that the civil part of the state administration has access to secure IT areas, including secure communications. The Swedish Fortifications Agency has analysed the conditions for establishing regional data clusters. At the government's behest, the Swedish Post and Telecom Authority has also submitted a proposal for an administration model to enable coordination of secure IT areas. Nevertheless, none of these proposals has yet been implemented.

Of course, it is a step in the right direction that the government has now commissioned an investigation relating to secure and cost-effective IT operation for the public administration.[123] However, it is our assessment that such proposals will require access to physical infrastructure that does not currently exist and will take several years to complete after a decision has been made. Therefore, we find that there is good reason for the government to begin, in parallel with ongoing enquiries, to implement the proposals that the Fortifications Agency and the Post and Telecom Authority have submitted. If this is not done, the implementation of a coordinated secure state IT operation will be delayed, with the risk of increased vulnerability in

[123] See dir. 2019:64.

public authority IT operations. In this connection, we also want to stress that a physically secure infrastructure, for example in the form of secure IT areas and communications, should not be limited to state authorities. It cannot be ruled out that municipal authorities and certain private entities also operate sustaining societal IT functions that should have the opportunity of an equivalent protection level.

Sweden's public organisations must work together to ensure that cloud services are offered on legal and appropriate terms

We are aware that the management of public cloud services that we are calling for would entail Swedish public authorities re-evaluating investments and strategic approaches that have already been undertaken. This also affects the Swedish Social Insurance Agency, which would need to review completed, ongoing and planned projects. In the meantime, we consider Sweden's security and the modus operandi of public authorities to be far too great an importance to be subordinated to considerations of investments that have already been made. The costs that Swedish society would ultimately suffer if we were unsuccessful in establishing protection of sustaining societal functions or of our citizens' privacy cannot be predicted. The dependency on services under the disadvantageous or even unlawful conditions that Swedish public authorities have already obtained or are in the process of obtaining, means it will be even more difficult to ensure that the services are provided under the conditions we want in the long term. Nevertheless, we believe that there is a solution to the problem, but that it must be found through collaboration in the public sector. With such coordination, the private providers will also obtain a clearer picture of the public sector's requirements, which will entail clearer financial incentives to make necessary adjustments to the services.

Swedish public authorities can act jointly

Cloud services entail great possibilities for meeting the general public's expectations for an effective and accessible public administration. If properly designed, they can also make a strong contribution to the public sector's ability to satisfy the government's ambitious call to make the best use of the opportunities presented by digitalisation.

However, the key words are 'properly designed'. The services that Swedish public authorities utilise must be adapted to the needs and security requirements of the public authorities rather than being based on existing solutions that private companies want to offer us. This demand for rapid digital development must not mean that we accept standard contractual clauses that do not fulfil the requirements in current legislation or otherwise fail to guarantee strong protection for security and privacy.

How can we achieve this? Here the Swedish Social Insurance Agency wants to highlight the fact that the Swedish public sector as a whole constitutes a relatively large purchasing entity and thus is in good position to make demands on the services to be procured. However, this is conditional on us taking action jointly – a collective state administration with a clear message for the market is difficult to disregard. By jointly formulating a set of requirements, we can do more than influence the existing market participants. We can also create opportunities for new participants who provide products that meet our requirements.

There is no lack of good models for this task. The Dutch government has successfully negotiated an addendum to Microsoft's standard agreement for Microsoft Office for the purpose of fulfilling the GDPR requirements. The Netherlands has an ambition to incorporate the entire EU public sector into the supplemental agreement. If Swedish public authorities combine forces in setting out our requirements, we should also be able to benefit from the progress made by the Netherlands. The Dutch initiative only solves part of the legal conflicts with respect to data protection. Therefore, Sweden should also, on both a national and agency level, join the initiatives for collaboration that are now developing between the public authorities of EU countries for the purpose of negotiating better contractual terms with the major service providers.[124] In this way we will increase the chances of the market providing services where the control is kept within the public authority rather than being transferred to private participants or third countries.[125] In the same way, we should be able to take action to ensure that private services are adapted to other Swedish legislation and to the security level that the Swedish public sector needs to demand in order to maintain control over its functions. In the Netherlands, the supplemental agreement was negotiated by a designated public authority with a collective responsibility to represent the interests of the Netherlands. We have everything to gain by coordinating our efforts in a similar manner.

Summary of our conclusions

In summary, it is the Swedish Social Insurance Agency's view that the Swedish debate on public authorities' conditions for utilisation of public cloud services provided by private market participants has not had the right focus. The Swedish Social Insurance Agency has determined that there are conflicting standards between the legislation of other countries on access to data stored by service providers and Swedish and EU law. However, the emphasis of the discussion should not be on whether the public authorities in these countries are exploiting the opportunity to gain access to information belonging to Swedish public authorities. Rather, appropriateness and the public authorities' collective responsibility to protect sustaining societal functions should serve as the basis of this debate.

In our judgement the use of public cloud services under private management in sustaining societal functions increases the overall vulnerability of these functions and the risk of unauthorised parties gaining access to data. Moreover, the use of such cloud services creates major - sometimes insurmountable - difficulties in background checks on the staff who will work with security-sensitive activities and in monitoring of concluded protective security agreements. In addition, the CLOUD act and similar legislation entail difficulties with respect to establishing fair consequence assessments or risk and vulnerability analyses. The fundamental problem of Swedish public authorities handing over control over data from their functions to private companies or other countries' public authorities is an additional factor.

Against this backdrop, the Swedish Social Insurance Agency will not transfer operation of such systems to private companies that are under the jurisdiction of a country having legislation like the CLOUD Act. The extent to which the

124 A notable example is the Hague Forum for Cloud Contracting, which will be staged again by the Strategic Vendor Management Unit of the Dutch Ministry of Justice and Security during the spring of 2020.

125 Such services could be carried out by a private cloud service installed on site with the client, which essentially means that the public authority buys a service that is used on the public authority's own servers.

procurement of services can take place with Swedish or European market participants may be determined on the basis of an appropriateness assessment in each case, wherein items such as the type of function, sensitivity of the information and possible terms of agreement are taken into account. Nevertheless, in the case of security-sensitive activities, for example, the Swedish Social Insurance Agency's goal for the future will be to keep our IT operation under state management.

In order for Swedish public authorities to be able to maintain an adequate protection level for digital information, the Swedish Social Insurance Agency has also determined that Sweden as a nation needs to discuss the meaning and value of digital sovereignty. A basis for these discussions should, in our opinion, be that our sustaining societal functions must be protected from attacks and that dependency on individual services on the market should be reduced. In this manner, we can manage the trust that we have been given by the citizens to take care of society's functions and the individual's sensitive personal data. We have thus concluded that it is now time for Sweden as a nation to make the transition from a passive approach to an active strategy for digital sovereignty, targeting what this entails for the daily functions of public authorities. This requires clear governance and a long-term plan of action that comprises the entire public sector. Such a plan of action should also include secure infrastructure, in the form of secure IT areas and secure communications, and a long-term sustainable administrative model for this infrastructure.

Such an approach does not have to mean that digitalisation of the public sector stops. We are certain that private and public innovators with the right resources and conditions can contribute to the Swedish public authorities continuing to benefit from all of the opportunities presented by digitalisation without risking the security of sustaining societal functions. Through collaboration on a national level and within the EU, Swedish public authorities can also ensure that the private services we choose to utilise are adapted to our needs, legislation and a security level that allows us to retain control over our functions and activities. This must always be based on the idea that the public authorities, not private companies, determine the conditions for the services that are procured.

References

Abelson Harold et al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, (MIT-CSAIL-TR-2015-026), November 2015

Access Now, European Digital Rights (EDRi), Electronic Frontier Foundation, Panoptykon Foundation, *Letter to US Congress*, 19-03-2018 https://edri.org/files/cross-borderaccesstodata/lettertocongress_CLOUDAct_20180319.pdf

Amnesty International USA, Electronic Frontier Foundation and Human Rights Watch et al.., Letter to American Congress, 12-03-2018. https://www.eff.org/document/coalition-letter-opposing-cloud-act (Retrieved 02-09-2019)

Auchard Eric Reuters, *Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV* , 20-03-2018 https://www.reuters.com/article/us-facebook-cambridge-analytica- kenya/cambridge-analytica-stage-managed-kenyan-presidents-campaigns-uk-tv-idUSKBN1GV300 (Retrieved 10-11-2019)

Autoriteit Persoonsgegevens (Dutch DPA), *Summary of Investigation Report Public Version Microsoft Windows 10 Home and Pro*, August 2017

AWS, *AWS Government cloud for the American state* https://aws.amazon.com/govcloud-us/ (Retrieved 10-09-2019)

AWS, *Global Infrastructures Regions and AZs* https://aws.amazon.com/about- aws/global-infrastructure/regions_az/?p=ngi&loc=2 (Retrieved 10-09-2019)

AWS, *Information Request Report*
https://d1.awsstatic.com/certifications/Information_Request_Report_June_2019.pdf (Retrieved 10-09-2019)

AWS *Protection Data using encryption*
https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html (Retrieved 10-11-2019)

Bellanger Pierre, *De la souveraineté en général et de la souveraineté numérique en particulier*, Les Échos, 30-08-2011.

Blix Fredrik and Brolin Richard, *Grönt ljus för kommuner, regioner och statliga myndigheter att överväga molntjänster [Green light for municipalities, regions and state authorities to consider cloud services]*, Cybercom Group, 04-07-2019 https://www.cybercom.com/sv/Om-Cybercom/Bloggar/digital-sakerhet/gront-ljus-for-kommuner-regioner-och-statliga-myndigheter-att-overvaga-molntjanster/ (Retrieved 04-09-2019)

Bondcap, *Internet Trends 2019* https://www.bondcap.com/report/itr19 (Retrieved 20-09-2019)

Bundesministerium des Innern, für Bau und Heimat, *BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung*, 19-09- 2019 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html (Retrieved 20-09-2019)

Bundesministerium für Wirstschaft und energie, *Digital Gipfel*
https://www.de.digital/DIGITAL/Navigation/DE/Service/Digital-Gipfel/Digital-Gipfel.html (Retrieved 20-09-2019)

Butler Brandon, *What is hybrid cloud computing? The benefits of mixing private and public cloud services, Networkworld,* 17-10-2017 https://www.networkworld.com/article/3233132/what-is-hybrid-cloud- computing.html (Retrieved 09-11-2019)

Cadwalladr Carole, *The Great British Brexit robbery how our democracy was hijacked, The Guardian,* 07-05-2017 *https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit- robbery-hijacked-democracy* (Retrieved 10-11-2019)

Corey Varma, *Encryption vs. Fifth Amendment* http://www.coreyvarma.com/2015/07/encryption-vs-fifth-amendment/ (Retrieved 17-09-2019)

Council of Bars and Law Societies of Europe, *CCBE Assessment of the U.S. CLOUD Act,* 28-02-2019

Daskal Jennifer, Unpacking the CLOUD Act, *EUCRIM, 31-01-2019* https://eucrim.eu/articles/unpacking-cloud-act/ (Retrieved 02-09-2019)

Department of Justice, Office of Public Affairs, *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online,* 03-10-2019 https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists (Retrieved 09-10-2019)

Digital Gipfel, Plattform Innovative Digitalisierung der Wirtschaft: Fokusgruppe Digitale Souveränität in einer vernetzten Gesellschaft, *Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen,* 2018 https://www.de.digital/DIGITAL/Redaktion/DE/Digital- Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche- intelligenz.pdf?_blob=publicationFile&v=5 (Retrieved 15-10-2019)

Director of National Intelligence, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 08-06-2013 https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf (Retrieved 03-09-2019)

Ds 2017:66, *Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025 [Resistance capacity - Alignment of the total defence and configuration of the civil defence 2021 - 2025]*

Ds 2018:6, *Study of the Swedish Transport Agency's procurement of IT services*

E-delegationen, Strategi för myndigheternas arbete med e-förvaltning [e-delegation, strategy for public authorities' work with e-administration] (SOU 2009:86)

E-delegationen, *Så enkelt som möjligt för så många som möjligt [*e-delegation, *as easy as possible for as many as possible]* (SOU 2011:67)

EDPB-EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection,* 10-07-2019

The Swedish National Financial Management Authority, *It-kostnadsmodell [IT cost model]*(2014:50), 01-10-2014

Electronic Frontier Foundation, *EFF and 23 Groups Tell Congress to Oppose the CLOUD Act,* 11-03-2018 https://www.eff.org/deeplinks/2018/03/eff-and-x-groups-tell-congress-oppose- cloud act (Retrieved 08-08-2019)

Electronic frontier Foundation, EFF in the United States Court of Appeals for the Eleventh Circuit Case: 11-12268

See Electronic Frontier Foundation, *The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom*, 09-04-2018 https://www.eff.org/de/deeplinks/2018/04/us-cloud-act-and-eu-privacy-protection- race-bottom#_ftn1 (Retrieved 07-08-2019)

eSam, *Kompletterande information om molntjänster* [eSam, *Complementary information on cloud services*] 20-09-2019

eSam, *Rättsligt uttalande om röjande och molntjänster [Legal statement on disclosure and cloud services]*, VER 2018:57, 23-10-2018

eSam, *Röjandebegreppet enligt offentlighets- och sekretesslagen, [The concept of disclosure according to the Public Access to Information and Secrecy Act]* VER 2015-190, 17-12-2015

The European Parliament, *The European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield* (2018/2645(RSP))

The European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* (PE 583.137)

The European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, adopted on 25 May 2018

European Commission, *Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp.*

The European Council, *A New Strategic Agenda for 2019-2024*, June 2019 https://www.consilium.europa.eu/media/39936/a-new-strategic-agenda-2019-2024- sv.pdf (Retrieved 01-10-2019)

The Council of the European Union (Transport, Telecommunications and Energy Council), *Conclusions on the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion"*, 07-06-2019, https://www.consilium.europa.eu/media/39667/st10102-en19.pdf

Federal Ministry for Economic Affairs and Energy (BMWi), *Criteria and catalogue for cloud services version 2*

Federal Ministry for Economic Affairs and Energy(BMWi), *Project GAIA-X A Federated Data Infrastructure as the cradle of a vibrant European ecosystem*

Federal Ministry for Economic Affairs and Energy (BMWi), *Trusted Cloud – Cloud providers* https://www.trusted-cloud.de/en/cloud-services (Retrieved 10-11-2019)

Fedramp, *Third Party Assessment Organization (3PAO)*

https://www.fedramp.gov/assessors/ (retrieved 20-09-2019) Ministry of Finance, *Appropriation Directions for the National Financial Management Authority 2014*

Ministry of Finance, *Uppdrag att erbjuda samordnad säker statlig it-drift [Commission to offer coordinated secure state IT operation]* (FI2017/03257/DF)

Ministry of Finance, *Uppdrag att föreslå en förvaltningsmodell för skyddade it- utrymmen [Commission to propose an administration model for protected IT areas]* (Fi2017/03084/DF)

Swedish National Defence Radio Establishment, *Årsrapport 2018 [Annual report 2018]*

Swedish Ministry of Defence, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter [Commission to establish a national cybersecurity centre]* Fö2019/01000/SUND, 26-09-2019

Swedish Armed Forces, *Godkända kryptoapparater September 2019 [Approved cryptography devices, September2019]* https://www.forsvarsmakten.se/sv/organisation/hogkvarteret/militara-underrattelse- och-sakerhetstjansten/kryptografiska-funktioner/ (Retrieved 01-10-2019)

Försvarsutskottets betänkande [The Defence Committee's perspective] 2014/15:FöU11

The Swedish Social Insurance Agency, *Delredovisning samordnad och säker statlig it-drift, [Interim report on coordinated and secure state IT operation]* (046278- 2017), 24-11-2017

The Swedish Social Insurance Agency, *Delredovisning samordnad och säker statlig it-drift, [Interim report on coordinated and secure state IT operation]* (046278- 2017), 29-10-2018

Gartner, Market Insight: *Finding Cloud Opportunities in the government,* 27-06-2017 ID: G00327356

Gellman Barton and Soltani Ashkan, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, The Washington Post, 2013-10-30* https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to- yahoo-google-data-centers-worldwide-snowden-documents- say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (Retrieved 24-09-2019)

Google, *Request for user information* https://transparencyreport.google.com/user-data/overview (Retrieved 05-09-2019)

Gutierrez, Natashya, *Did Cambridge Analytica use Filipinos' Facebook data to help Duterte win?, Rappler,* 05-04-2018 https://www.rappler.com/nation/199599-facebook-data-scandal-cambridge- analytica-help-duterte-win-philippine-elections (Retrieved 10-11-2019)

Hellberg, Islam, Karlsson, *Säkerhet vid molnlösningar [Security for cloud solutions]*, Örebro University and the Swedish Civil Contingencies Agency

Hern Alex, *Facebook agrees to pay fine over Cambridge Analytica scandal, The Guardian,* 30-10-2019 https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal (Retrieved 10-11-2019)

Huizing Lennart, *The Hague Forum for Cloud Contracting,* Privacy Company, 2019-10-24 https://www.privacycompany.eu/en/the-hague-forum-for-cloud-contracting/ (Retrieved 02-10-2019)

The Ministry of Infrastructure, *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen [Secure and cost-efficient IT operation for public administration]* (Dir. 2019:64)

Ministry of Infrastructure, *Uppdrag att erbjuda samordnad säker statlig it-drift [Amendment to commission to offer coordinated secure state IT operation]* (I2019/02515/DF)

The Privacy Committee, *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén [What is the privacy situation? - A survey by the Privacy Committee]* (SOU 2016:41)

International Organization for Standardization, ISO/IEC 2382:2015(en) Information technology — Vocabulary

The Ministry of Justice, proposal referred to the Council on Legislation for consideration *Hemlig dataavlyssning [Secret data surveillance]*, 24-10-2019

The Ministry of Justice, *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor [Commission for the Swedish Civil Contingencies Agency to implement purposeful training in the field of information security for the public sector]* (Ju2019/03057/SSK)

The Ministry of Justice, *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen [Commission for the Swedish Civil Contingencies Agency to develop a structure for follow-up of systematic information security work in public administration]* (Ju2019/03058/SSK, Ju2019/02421/SSK)

The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Preliminary Study Report on Web-based Office Support]*, Ref. 23.2-6283-18, 22-02-2019

Kristiansson Stefan, *Om underrättelsehotet mot Sverige, [The Intelligence Threat against Sweden]*, Frivärld Report no. 7 2019.

Le ministère de l'Europe et des Affaires étrangères, *Déclaration du conseil franco-allemand de sécurité et de défense, 2015* https://www.diplomatie.gouv.fr/IMG/pdf/_16-04-07_declaration_cfads cle8eaec8.pdf

Markander Mikael, *Strömavbrott hos molnjätten – kunder förlorade data [Power Failure at Cloud Giant - customers lost data]*, ComputerSweden,06-09-2019 https://computersweden.idg.se/2.2683/1.723105/kunder-drabbade-stromavbrott- aws (Retrieved 10-09-2019)

Maurer Tim et al.*Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013,* New America's Open Technology Institute and the Global Public Policy Institute (GPPi) https://www.gppi.net/media/Maurer- et-al_2014_Tech-Sovereignty-Europe.pdf

Microsoft, the Swedish Association of Local Authorities and Regions et al, Open seminar at Almedalen 2019, CLOUD ACT - helpful or not https://www.youtube.com/watch?v=tqCRZt81bZk (Retrieved 04-09-2019)

Microsoft, *Configure ADRMS restrictions* https://docs.microsoft.com/sv-se/azure/information-protection/configure-adrms-restrictions (Retrieved 23-09-2019)

Microsoft, *Konfigurera diagnostikdata för Windows i din organisation, [Configure diagnostic data in your organisation]* 2019 https://docs.microsoft.com/sv-se/windows/privacy/configure-windows-diagnostic- data-in-your-organization (Retrieved 24-09-2019)

Microsoft, *Law Enforcement Requests Report* https://www.microsoft.com/en- us/corporate-responsibility/lerr (Retrieved 10-09-2019)

Microsoft *Cloud Services and Security* 13-12-2018 https://news.microsoft.com/sv-se/2018/12/13/molntjanster-och-sakerhet/ (Retrieved 04-09-2019)

AWS, *Office 365 Government cloud for the American state* https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365- platform-service-description/office-365-us-government/office-365-us-government (Retrieved 23-09-2019)

Microsoft, *Service encryption with Customer Key for Office 365 FAQ*, 2018-07-31 https://docs.microsoft.com/en-us/office365/securitycompliance/service-encryption- with-customer-key-faq (Retrieved 24-09-2019)

Microsoft, Bring your own key (BYOK) information about Azure Information Protection, *22-09-2019* https://docs.microsoft.com/sv-se/azure/informationprotection/byok-price-restrictions (Retrieved 25-09-2019)

Ministerie van Justitie en Veiligheid, *Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft* (Ons kenmerk 2635551), 01-07-2019

Ministry of Justice and Security Strategic Vendor Management Microsoft, DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data

The Swedish Civil Contingencies Agency, *Vägledning för identifiering av samhällsviktig verksamhet [Guidelines for identifying vital societal functions]*, MSB597, December 2013

The Swedish Civil Contingencies Agency, Upphandling till samhällsviktig verksamhet – en vägledning [Procurement for vital societal functions - guidelines], MSB1275, September 2018.

The Swedish Civil Contingencies Agency, Vägledning för identifiering av samhällsviktig verksamhet [Guidelines for identifying vital societal functions, MSB1408, June 2019

The Swedish Civil Contingencies Agency, *Vägledning för risk- och sårbarhetsanalyser, [Guidelines for risk and vulnerability analyses]* MSB245, April 2011

The Swedish Civil Contingencies Agency, *Övergripande inriktning för samhällsskydd och beredskap, [General alignment for civil defence and readiness]* MSB708, June 2014

Ministry of Enterprise and Innovation, *Med medborgaren i centrum – Regeringens strategi för en digitalt samverkande statsförvaltning [With a focus on the citizen – Government strategy for digitally collaborative state administration]* (N2012:37)

Office of the Director of National Intelligence United States Intelligence Activities (Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008))

The Swedish Pensions Agency, *Molntjänster i staten – en ny generation av outsourcing (med bilagan Juridisk analys av myndigheters informationshantering i molnet) [Cloud services in the state - a new generation of outsourcing (with the annex legal analysis of public authorities' management of information in the cloud)]*, 2016

The Swedish Post and Telecom Authority, *Förslag till en förvaltningsmodell för skyddade it-utrymmen [Proposal for an administration model for protected IT areas] (Ref. no.:* 17-8280)

Government bill 2014/15:109, *Försvarspolitisk inriktning – Sveriges försvar 2016-2020 [Defence policy alignment - Sweden's defence 2016-2020]*

Government bill 2019/20:15, *Skydd av Sveriges säkerhet vid radioanvändning [Protection of Sweden's security when radio transmitters are used]*

Punke Michael, AWS and the CLOUD Act, *AWS Security Blog*, 27-05-2019 https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/ (Retrieved 02-09-2019)

The Government *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen [Secure and cost-efficient IT operation for public administration]* (Dir. 2019:64

Report of the Government of Sweden 2010/11:138, The Swedish National Audit Office's audit of IT within state administration and state IT projects

Minutes of the Swedish Parliament 2014/15:117

The Swedish National Audit Office, *Granskning om IT-förvaltning delvis missförstådd, [Audit of IT administration partially misunderstood]*, 26-09-2017 https://www.riksrevisionen.se/om-riksrevisionen/kommunikation-och-media/nyhetsarkiv/2017-09-26-granskning-om-it-forvaltning-delvis- missforstadd.html (Retrieved 30-09-2019)

The Swedish National Audit Office, *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet? [IT within state administration - have the public authorities adequately evaluated the question of whether outsourcing contributes to increased effficiency]* (RiR 2011:4)

National Government Service Centre, *En gemensam statlig molntjänst för myndigheternas it-drift - Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner [A common state cloud service for IT operations of public authorities] – periodic report on the Government mandate on coordination and relocation of public agency activities,* (Ref.10052- -2016/1121), 07-02-2017

Strategic Vendor Management Microsoft for the Dutch Government and Ministerie van Veiligheid en Justitie, *EU Software and Cloud Supplier Customer Council* https://www.youtube.com/watch?v=96EVKaosVps&feature=youtu.be (Retrieved 25-09-2019)

The Swedish Association of Local Authorities and Regions, *Molntjänster och konfidentialitetsbedömning, [Cloud services and confidential assessment],* https://skl.se/download/18.3414859716e267c4fe2ad9d8/1572961426896/Molntja%CC%88nster%20och%20konfidentialitetsbedo%CC%88mning_191105.pdf (Retrieved 09-11-2019)

The Swedish Association of Local Authorities and Regions, *Ställningstagande om informationshantering i vissa molntjänster [Position on information management in certain cloud services],* ref. no. 19/00087, 12-04-2019

The Swedish Security Service, *Informationssäkerhet [Data Security]* https://www.sakerhetspolisen.se/sakerhetsskydd/informationssakerhet.html (Retrieved 05-09-2019).

The Swedish Security Service, Personalsäkerhet [Personal Security] https://www.sakerhetspolisen.se/sakerhetsskydd/personalsakerhet.html (Retrieved 05-09-2019).

The Swedish Security Service, *Säkerhetsskydd vid upphandlingar och affärsavtal*

[Security protection for procurement processes and commercial agreements] https://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsskydd-vid- upphandlingar-och-affarsavtal.html (Retrieved 06-09-2019)

The Swedish Security Service, *Vägledning i säkerhetsskydd – Introduktion till protective security [Guidelines for protective security - Introduction to security protection]* https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64d/1560777315837/Vagledning-Introduktion-till-sakerhetsskydd.pdf (Retrieved 05-09-2019)

The Swedish Security Service, Vägledning i säkerhetsskydd – *personalsäkerhet Årsbok 2017 [Guidelines for protective security – personnel security, 2017 Annual Report]*

Swedish Security Service, *Årsbok [Annual Report]* 2018, p.

The App Association et al., *Open letter to Attorney General Barr*, 21-06-2019 Https://www.bsa.org/files/policy-filings/06212019bsaletteruseulea.pdf (Retrieved 02-09-2019)

Swedish Defence Research Agency and the Swedish Fortifications Agency, *Strategisk utblick 8 – Totalförsvarets tillväxt –utmaningar och möjligheter, Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster, [Strategic outook 8 - Growth of Swedish total defence - challenges and opportunities, How we can protect Sweden's security-sensitive IT services]* (FOI 4773), May 2019

The Swedish Transport Agency, *Kartläggning av hanteringen av vissa uppgifter [Survey of the management of certain data]* (TSG 2017- 2515), 23-01-2018

United States Department of commerce, *Security and Privacy Controls for Federal Information Systems and Organizations* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Retrieved 15-10-2019)

United States Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,* White Paper, April 2019

United States District Court for the District of Vermont., No. 2:06-mj-91, 2009 WL 424718 Feb. 19, 2009. MEMORANDUM of DECISION In re Grand Jury Subpoena to Sebastien Boucher

Utredningen om hemlig dataavläsning [Investigation on secret data surveillance], *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, [Secret data surveillance - an important tool in the fight against serious crime]* (SOU 2017:89)

Study on IT crime convention, The Council of Europe Convention on IT-Related Crime (SOU 2013:39)

von der Leyen Ursula, *Political Guidelines for the Next European Commission*, 2019-2024

Annex 1 Outsourcing of governmental IT services – a historical overview

The proposal for the government to place a requirement on the public authorities to develop a strategy for their provision of IT services, a 'sourcing strategy', had already been highlighted in the e-delegation's initial report in 2009. The strategy would take into account the public authorities' specific situations. The parameters that would determine the choice of sourcing were primarily cost, quality and flexibility.[126]

In 2011, the Swedish National Audit Office conducted an analysis of whether state authorities were giving sufficient consideration to outsourcing to satisfy the needs of IT.[127] The National Audit Office's conclusion was that outsourcing had not been adequately investigated. The reason indicated was that public authorities cannot report their IT costs, that there are deficiencies in internal control, that there is a lack of requirements for efficiency in the IT departments of public authorities, that expertise within purchasing is low, that there are uncertainties with respect to data classification of 'sensitive information', that the sharing of knowledge between public authorities is deficient and that the government has not facilitated outsourcing of services. Consequently, the National Audit Office recommended establishing guidelines and an increased exchange of experience between public authorities.[128]

In its response to the report, the government indicated that the issue of public authorities outsourcing IT services would be further developed. The government also indicated that it was desirable that a greater part of the public authorities' IT needs should be satisfied by outsourcing of services.[129]

The National Audit Office later commented that the interpretation of their investigation had been partly misunderstood in connection with the discussions following the outsourcing of IT services by the Swedish Transport Agency.[130]

In the government's 2012 digitalisation strategy, it was stated that in 2012-2013 the e-delegation would conduct an in-depth preliminary study.[131] The e-delegation described the purpose of the preliminary study as the identification and description of the possibilities for improved efficiency of the public authorities' IT operation across ministerial and authority boundaries, including proposals for how such solutions can be designed. The preliminary study would shed light on how the state should operate, replace or buy and sell IT services within the state sector, including

126 *E-delegationen, Strategi för myndigheternas arbete med e-förvaltning [e-delegation, strategy for public authorities' work with e-administration]* (SOU 2009:86) pp. 15 et seq.

127 Off-shoring is a term that is used for outsourcing when the IT service provision takes place in another country.

128 The Swedish National Audit Office, *IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet? [IT within state administration - have the public authorities adequately evaluated the question of whether outsourcing contributes to increased efficiency?]* (RiR 2011:4), p. 63 et seq.

129 *Report of the Government of Sweden 2010/11:138, [The Swedish National Audit Office's audit of IT within state administration and state IT projects]*

130 The Swedish National Audit Office, *Granskning om IT-förvaltning delvis missförstådd [Audit of IT administration partially misunderstood]*, 26-09-2017

131 Ministry of Enterprise and Innovation, *Med medborgaren i centrum – Regeringens strategi för en digitalt samverkande statsförvaltning [With a focus on the citizen – The government's strategy for digitally collaborative state administration]* (N2012:37), p. 22

evaluation of various sourcing models. It would also highlight the requirements for information security and include an analysis of obstacles and recommendations for implementation strategies.[132] Nevertheless, the preliminary study report was never published.

In 2014 the Swedish government commissioned the National Financial Management Authority with the task of developing public authorities' work related to IT costs, IT investments and outsourcing and the government reported in the annual report that the issue of sourcing strategy should thus be considered as being in the final stages of preparation at the Government Offices.[133] The National Financial Management Authority's commission was to produce an IT cost model. The authority should also consider how the model can incorporate monitoring of strategic choices, as well as a strategy for IT provision.[134] The National Financial Management Authority's 2014 report described the state's costs for IT.[135]

In parallel with the National Financial Management Authority's commission, the Swedish Pensions Agency was commissioned by the government in 2015 to analyse and evaluate the potential for the use of cloud services in the state and to outline what risks and obstacles may be associated with the use of cloud services in state activities. The analysis should also show how use of cloud services can contribute to the objective of simpler, more open and more efficient administration. The Swedish Pensions Agency stressed in its report that cloud services carry certain limitations for the state's activities and that the more sensitive the information was and the more integrations there were in place, the more difficult outsourcing became. Each authority was recommended to carry out a legality check and to ensure that good information security can be maintained.[136] The legal aspects were shown in a special appendix. The Swedish Pensions Agency highlighted the question of national security and stressed that it required further attention. Consequently, the Swedish Pensions Agency also recommended an ongoing assessment of state cloud services.[137]

The National Government Service Centre was commissioned by the government in 2016 specifically to analyse the possibilities of state cloud services. The report was submitted in February 2017. The National Government Service Centre's conclusion was that the majority of state authority IT operation should be coordinated in a state cloud service which would offer the authorities two services: computing power and storage.[138]

132 *e-delegationen, Så enkelt som möjligt för så många som möjligt [e-delegation, as simple as possible for as many as possible]* (SOU 2011:67), p. 30

133 The Ministry of Finance, *Årsredovisning för staten 2012 [2012 State Annual Report]*, p. 115, Ministry of Finance, *Årsredovisning för staten 2013[2013 State Annual Report]*, p. 116 and The ministry of Finance, *Årsredovisning för staten 2014, [2014 State Annual Report]*, p. 124.

134 Ministry of Finance, *Regleringsbrev för Ekonomistyrningsverket [Appropriation directions for National Financial Management Authority] 2014*, p. 5

135 The Swedish National Financial Management Authority, *It-kostnadsmodell [IT cost model]* (2014:50)

136 The Swedish Pensions Agency, *Molntjänster i staten – en ny generation av outsourcing, 2016 [Cloud services in the state - a new generation of oursourcing, 2016]*, p. 73 et seq.

137 The Swedish Pensions Agency, *Molntjänster i staten – en ny generation av outsourcing, 2016 [Cloud services in the state - a new generation of oursourcing, 2016]*, Annex *Juridisk analys molntjänster i staten [Legal analysis of cloud services in the state]*, p. 58 et seq.

138 National Government Service Centre, En gemensam statlig molntjänst för myndigheternas it-drift - Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner [A joint state cloud services – periodic report on the government mandate on coordination and relocation of public agency activities, (Ref.10052- -2016/1121)

In 2017 the government commissioned the Swedish Post and Telecom Authority with the task of developing a proposal for an administration model for protected IT areas.[139] The Swedish Post and Telecom Authority submitted a final report in February 2018 and recommended an in-depth analysis followed by implementation of an administration model that would enable coordinated securing of IT areas.[140]

The Swedish Post and Telecom Authority's commission was supplemented in August 2017 with an assignment for the Swedish Social Insurance Agency to offer coordinated secure state IT operation for suitable functions and public authorities from 2017 to 2020.[141] The Swedish Social Insurance Agency should also draft a proposal for suitable designs for the coordination of state IT operation after 2020. The Swedish Social Insurance Agency stressed in its interim reports in 2017 and 2018 that the need for support with respect to IT operation is a major one for state authorities and especially smaller agencies have need of a total undertaking.[142] In its 2018 follow-up report, the Swedish Social Insurance Agency stressed the importance of implementing the administration model for secure IT areas that the Swedish Post and Telecom Authority proposed in 2018.[143]

The Swedish Fortifications Agency conducted a number of preliminary studies from 2016-2019 with respect to access to IT areas with fortification. A preliminary study financed by MSB analysed a broader need from the state administration to enable coordinated IT services. After the preliminary study was completed, the Fortifications Agency determined that a significant part of the Swedish total defence capability involves protection of vital societal activities, not least for vital societal IT systems.[144]

In September 2019, the government presented measures for strengthening data and cybersecurity. A decision was made to establish a national cybersecurity centre for the purpose of strengthening Sweden's collective ability to prevent, discover and manage cyber threats. The Swedish Civil Contingencies Agency was commissioned with the task of implementing targeted training initiatives in the area and developing

139 Ministry of Finance, *Uppdrag att föreslå en förvaltningsmodell för skyddade it-utrymmen [Commission for proposing an administration model for protected IT areas] (Ref. Fi2017/03084/DF*)

140 The Swedish Post and Telecom Authority, *Förslag till en förvaltningsmodell för skyddade it-utrymmen [Proposal for an administration model for protected IT areas]* (Ref: 17- 8280)

141 The Ministry of Finance, *Uppdrag att erbjuda samordnad och säker statlig it-drift [Commission to provide coordinated and secure state IT operation]* (Fi2017/03257/DF)

142 A total undertaking entails access to an external IT department that handles development, administration and operation in the same manner in which an internal IT department would. See the Swedish Social Insurance Agency, *Delredovisning samordnad och säker statlig it-drift, [Preliminary on coordinated and secure state IT operation]* (046278-2017), 24-11-2017 and *Delredovisning samordnad och säker statlig it-drift, [Preliminary on coordinated and secure state IT operation]* (046278-2017), 29-10-2018

143 The Swedish Post and Telecom Authority, *Förslag till en förvaltningsmodell för skyddade it-utrymmen [Proposal for an administration model for protected IT areas]* Ref. no.: 17-8280

144 Swedish Defence Research Agency and the Swedish Fortifications Agency, *Strategisk utblick 8 – Totalförsvarets tillväxt –utmaningar och möjligheter, Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster, [Strategic outlook 8 - Growth of Swedish Defence - challenges and opportunities, How we can protect Sweden's security-sensitive IT services]* (FOI 4773), May 2019

a structure for follow-up of the systematic data security work in the public administration.[145]

This commission was supplemented by the government's initiative to add an assessment with respect to secure and cost-effective IT operation for the public administration. According to the directive, the purpose of the assessment is to establish better conditions for the public administration to gain access to secure and cost-effective IT operation through either coordinated state IT operation or clearer legal conditions in order to be able to contract private providers of IT operation. In the directive, the government also identifies the lack of security in the matter of the legal conditions for outsourcing, primarily with respect to the interpretation of when information should be considered as having been disclosed according to secrecy legislation. The government confirms that this concern has become more acute in light of the CLOUD Act. The government has determined that release of data, including personal data, requires that the outsourcing authority also ensures that the processing of personal data will take place in compliance with the data protection regulation. The government also identified that a special challenge for an outsourcing authority might be to assess whether the supplier is able to provide adequate guarantees that it will implement suitable technical and organisational measures so that the processing fulfils the requirements in the Data Protection Act, that the data subject's rights are protected and that information is not impermissibly transferred to a third country, i.e. a country outside the EU and EEA territory.[146]

In the context of defining the committee directive, the government also decided to extend the Swedish Social Insurance Agency's commission to offer coordinated secure state IT operation. In such a way the government intended that the running time of the Swedish Social Insurance Agency's commission would be better aligned with the period of the newly added investigation and the time needed for subsequent action following the recommendations from the study.[147]

145 The Ministry of Justice, *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor, [Commission for the Swedish Civil Contingencies Agency to implement targeted data security training initiatives for the public sector]* (Ju2019/03057/SSK), The Ministry of Justice, *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen [Commission for the Swedish Civil Contingencies Agency to develop a structure for follow-up of systematic information security work in public administration]* (Ju2019/03058/SSK, Ju2019/02421/SSK) and the Ministry of Defence, *Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter [Commission to establish a national cybersecurity centre]* (Fö2019/01000/SUND)

146 The Ministry of Infrastructure, *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen [Secure and cost-efficient IT operation for public administration]* (Dir. 2019:64)

147 The Ministry of Infrastructure, *Ändring av uppdrag att erbjuda samordnad och säker statlig it-drift [Amendment to commission to provide coordinated and secure state IT operation]* (I2019/02515/DF)

Annex 2 The term cloud services and an estimate of the use of public cloud services in the Swedish public sector

Cloud services may be defined in a number of ways. In this report we use the definition from ISO/IEC 17788:2014 (ISO, 2014) where cloud services are defined as

"one or more capabilities offered via cloud computing […] invoked using a defined interface." While a cloud-based computer service is "a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Examples of resources in this definition include servers, operating systems, networks, software, applications, and storage equipment."[148]

The main features (characteristics) that ISO and SIS have defined and which additionally delineate the term are listed below:

- The users can access physical and virtual resources from various locations using different clients and units as long as there is an available network.
- The customers only pay for the resources that they use.
- Physical or virtual resources are divided in a manner such that several users share the environment, but their computations and data are isolated from and inaccessible to one another.
- The services give the users the possibility of doing what they need to do when they need to do it without requiring additional human user interactions or administrative expenses. In some cases, cloud services can be ordered, configured and used entirely without human interaction.
- Physical or virtual resources can be delivered swiftly and elastically, sometimes automatically, so that the resources can be expanded or contracted quickly and where the perceived customer benefit is to not have to worry about limitations to resources or capacity for planning.
- Cloud service providers can support simultaneous use by multiple parties while they use abstraction as a way of concealing the complexity in the process for customers.

Cloud services can be offered to different customer groups. In the event that the cloud services can only be made accessible to one customer (which might be the company providing the service), the cloud service is referred to as a private cloud service (private cloud). In this context, the word private is not used to describe the service provider's legal status. A cloud service that is offered to a limited group of customers is called a partner or community cloud service (partner cloud/community cloud), whereas a cloud service that is offered to a larger group or the general public is called a public cloud service (public cloud). However, it is important to stress that 'public' in this context does not mean that the general public has access to all data in the service, rather that

[148] ISO/IEC 17788:2014 is the international standard that provides an overview of what cloud services entail, partly including a recommendation of terminology and definitions to use in this context. See Hellberg et al., *Säkerhet vid molnlösningar [Security for cloud solutions]*

each customer has access to 'their' data only. There are examples of all three types of cloud services in Swedish state administration. The Swedish Social Insurance Agency, for example, uses private cloud services to offer certain functions to internal staff. Within the scope of the task commissioned by the government entitled 'Samordnad säker statlig it-drift' [Coordinated, Secure State IT Operation] the public authorities with which the Swedish Social Insurance Agency has initiated cooperation are offered certain services via partner cloud services. Many public authorities also use public cloud services like Office 365 in order to provide office support. In this context, term *hybrid cloud* may also be mentioned, referring to when several models are used in complement to one another in order to provide services to one customer.[149]

There are three internationally established types of cloud services that describe three different functional areas.

Infrastructure as a Service (IaaS) means the IT infrastructure services over the Internet. The customer can create and use resources of one or multiple cloud service providers in the form of physical hardware, such as servers, networks, storage spaces, architectural structures, load balancing, computing, etc. The customer themselves provides the platforms and applications that are run in the infrastructure. The customer does not have control over the underlying infrastructure but has control over operating systems, storage and applications developed and rolled out in the infrastructure, and so on.

Platform as a Service (PaaS) means that the provider provides application platforms via internet or other network in which users can install their own applications. An example of a PaaS is a development environment as a service.

Software as a Service (SaaS) means that the provider provides software as a service, i.e. finished or configurable applications via internet or other networks. This service type is sometimes called Applications as a Service (AaaS). This type of service can be delivered in several ways and can be accessible via a web browser. The provider is responsible for all maintenance.[150]

According to the study conducted by the Swedish Pensions Agency in 2016, SaaS solutions were by far the most commonly used model[151] and there is no indication that this has changed.

Since benefits are enjoyed by the customer and provider alike, cloud services have become an increasingly common delivery model. Cloud services are now used on a global level to handle an estimated 22 % of all organisational data. This development has progressed very quickly and within a few years cloud services may be used globally for larger amounts of data than are stored locally or internally on dedicated servers.[152]

Three American companies hold a very strong position in the market for cloud services. Amazon Web Services (AWS), Microsoft and Google offer public cloud services. These companies offer a wide range of public cloud services to both private individuals and larger organisations. The pace of growth is high and the combined profits for these three services stood at almost $47 billion in the first quarter of 2019.[153]

149 Butler, *What is hybrid cloud computing? The benefits of mixing private and public cloud services*

150 The Swedish Pensions Agency, *Molntjänster i staten [Cloud Services in the State]*, p. 13 et seq.

151 See the Swedish Pensions Agency, *Molntjänster i staten [Cloud Services in the State]*, p. 56 et seq

152 Bondcap, *Internet Trends 2019*, p. 153

153 Bondcap, *Internet Trends 2019*, Control into p. 116

A number of larger providers, including AWS and Microsoft, have established special private cloud services for American public authorities.[154] The purpose of this is to meet the requirements that American authorities present to their providers.[155] Equivalent strategies are in place in several countries for the purpose of ensuring that sovereignty can be protected.[156]

The use of cloud services by Sweden's public authorities is also on the rise. In a study financed by the Swedish Civil Contingencies Agency in 2018, 75% of the municipalities and public authorities surveyed indicated that they used at least one procured cloud service. Among municipal authorities, more than 80% used at least one public cloud service.[157]

The reason indicated most often was high flexibility, but cost benefits were also identified as important to more than half of the respondents.[158]

For municipalities, education administration was indicated as being the most common service, whereas state authorities indicated greater diversity in the type of service.

The respondents were also given the opportunity to indicate the obstacles hindering them from using cloud services. The primary reasons were deficient control and legislation. More than 20% indicated that they were on the verge of starting to use these services.[159]

Many of the public cloud services are successful based on the fact that customers and users are located around the world and must have access around the clock, every day of the year. In order to meet these demands, facilities and personnel are normally spread throughout various locations around the globe. The exact locations of different facilities and personnel are normally trade secrets, but certain information is publicly accessible. For example, AWS indicates that they are located in the USA, Brazil, Sweden, France, Germany, Denmark, Finland, the United Kingdom, Norway, Italy, the Czech Republic, Austria, Poland and Switzerland, South Africa, the United Arab Emirates, Israel, India, Hong Kong, China, Malaysia, the Philippines, Japan, Korea, Singapore and Taiwan, as well as in Australia.[160]

Determining the country whose law is applicable becomes a challenge when data owners, stored data and technical personnel who can gain access to said data are located in different countries. One thing that illustrates this is the debate related to the possibilities for law enforcement authorities to gain access to data in public cloud services.

154 Microsoft, *Microsoft Office 365 Government cloud* for the American state and AWS, *AWS Government cloud for the American state.* Not all American public authorities use these cloud services and several American public authorities use the public cloud services that these companies offer.

155 Fedramp, *Third Party Assessment Organization (3PAO) and United States Department of commerce, Security and Privacy Controls for Federal Information Systems and Organizations*

156 Gartner, *Market Insight: Finding Cloud Opportunities in Government,* ID: G00327356, 27-06-2017

157 Hellberg et al., *Säkerhet vid molnlösningar [Security for cloud solutions]*, p. 25

158 Hellberg et al., *Säkerhet vid molnlösningar [Security for cloud solutions]*, p. 28

159 Hellberg et al., *Säkerhet vid molnlösningar [Security for cloud solutions]*, p. 33

160 AWS, *Global Infrastructures Regions and AZs*

Annex 3 Conflicts between third-country legislation, EU law and national law

A major part of the Swedish debate surrounding the CLOUD Act and similar legislation has revolved around the conflicts between standards that arise between such legislation on the one hand and EU law and Swedish law on the other. This annex outlines the discussions that have been held in the areas of public access to information and secrecy, as well as data protection.

Public access to information and secrecy

Public Access to Information and Secrecy Act (OSL) – An overview

The constitutional right of access to public documents is delineated by the Swedish Public Access to Information and Secrecy Act (OSL) (2009:400).[161] If a piece of information is secret, it is prohibited to disclose it, either verbally, by releasing a public document or in another manner.[162] The prohibition against disclosing the document applies to public authorities as well as to a person who has gained knowledge of information because they participate in a public authority's activities, being employed by or commissioned by a public authority and so forth.[163] Secrecy functions as the overriding rule not only with respect to individuals, but also between public authorities and in relations with foreign public authorities and organisations.[164]

Of particular interest in relation to the CLOUD Act and other similar legislation is the possibility of disclosing confidential information to foreign public authorities. Such disclosure must only take place in accordance with legal regulations or ordinances or if the information would have been disclosed to a Swedish public authority in an equivalent situation. In the latter case, there is also the requirement that the disclosing authority checks to determine whether it is consistent with Swedish interests that the information be disclosed to foreign public authorities.[165]

However, there are special provisions for overriding secrecy. These may enable a disclosure of information that would otherwise be confidential if, for example, it is necessary for the public authority to perform their tasks or to satisfy legitimate needs of an individual.[166]

Before a Swedish authority makes confidential information available to a service provider, the authority must, among other things, analyse whether it entails disclosure of information in the sense set out in the Swedish Public Access to Information and Secrecy Act. The public authorities must also constantly ensure that secrecy rules are observed. Therefore, public authorities must be prepared for the

161 ch. 2 §§ 1-2 TF

162 ch. 3 § 1 OSL

163 ch. 2 § 1 OSL

164 ch. 8 §§ 1-3 OSL

165 ch. 8 § 3 OSL

166 Provisions overriding secrecy, which override all secrecy or secrecy according to a whole host of secrecy provisions are provided in ch. 10. of OSL. There are also provisions overriding secrecy in connection with the provision or provisions relating to secrecy in section IV and V of OSL.

introduction of new regulations, including in other countries, that affect the IT solutions that Swedish public authorities have chosen to use.[167]

The Conflict between legislation similar to the CLOUD Act and the Swedish Public Access to Information and Secrecy Act (OSL)

In 2015 the e-collaboration programme's legal expert group (referred to hereinafter as eSam) stated that information should not ordinarily be considered as disclosed in the sense of the Swedish Public Access to Information and Secrecy Act even if it has been made technically accessible for a service provider if

- the service provider is contractually obliged to refrain from viewing or transferring the information and
- the surrounding circumstances make it unlikely that this will take place anyhow.[168]

Because of the CLOUD Act and similar legislation, eSam issued a new legal statement in 2018. This statement took specific aim at the concept of disclosure with the use of cloud services that are subject to foreign legislation. eSam concluded that confidential information may be considered as disclosed if it is made technically accessible for a service provider who, as a consequence of the owner relationship, is bound, say, to regulations in another country by which the service provider may be obliged to transfer information without recourse to international legal aid or another legal basis under Swedish law. eSam made the assessment that in such situations it cannot be considered unlikely that the information will be transferred to third parties. The same assessment was made for the situations where the ownership situations or geographic location of a service provider's technical resources give cause to fear that human rights (such as protection of private life) or the interests of the general public (such as national security) would not be protected if Swedish public authorities' data had been made accessible to the service provider.[169]

eSam commented in September 2019 on its legal statement and indicated, to put it simply, the folllowing: In an initial step, the legal regulation of the parties' dealings must have been arranged in a sustainable manner. There must be a legally binding and sanctioned contractual confidentiality and the supplier must not be bound by regulations of foreign law to disclose information without a prior confidentiality review or another legal basis for disclosure according to Swedish law. If there are shortcomings in this, it means that making the information accessible to the provider should be considered as disclosure in the sense of the Swedish Public Access to Information and Secrecy Act. Then a probability assessment is not applicable. On the other hand, if a public authority determines that planned outsourcing would have a solid legal basis, an assessment is done to determine whether it is unlikely that the service provider or their personnel, who are not permitted to view or transfer the information, will handle the information in an impermissible manner anyway.

167 Refer also to The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Preliminary Study Report on Web-based Office Support],* Ref. 23.2-6283-18, 22-02-2019, p. 35.

168 eSam, *Röjandebegreppet enligt offentlighets- och sekretesslagen, [The concept of disclosure according to the Public Access to Information and Secrecy Act]* VER 2015-190, 17-12-2015

169 eSam, *Rättsligt uttalande om röjande och molntjänster [Legal statement on disclosure and cloud services]*, VER 2018:57, 10-23-2018.

The Legal, Financial and Administrative Service Agency agreed with eSam's assessment in 2019.[170] Moreover, the Legal, Financial and Administrative Services Agency indicated that it is inconsistent with the Swedish Public Access to Information and Secrecy Act for a service provider commissioned by a Swedish authority to disclose confidential information to a foreign authority pursuant to the CLOUD Act or similar legislation. Basically, this is due to the fact that there is no specific legal or regulatory provision authorising such disclosure. Moreover, it is not possible to ensure that it would have been permissible to disclose information to a Swedish authority in an analogous case or to ensure that Swedish interests are respected.[171] The Legal, Financial and Administrative Services Agency also noted that a Swedish authority that allows companies subject to regulations like the CLOUD Act to handle confidential information, will be viewed as prioritising the foreign regulation over Swedish legislation.[172]

Microsoft is one of the parties that has a different viewpoint. The company argues that the CLOUD Act entails even clearer reasons that it should be considered unlikely that a service provider contracted by Swedish public authorities would view or transfer confidential information. Therefore, Microsoft argues that 'automatic disclosure' does not take place in these situations and asserts that it is not merely the foreign ownership that should be decisive, rather that a more nuanced assessment must be made based on the contractual commitments, history and technical architecture. Microsoft also stresses that the number of cases where the company has received a request to hand over information that is stored outside the USA's borders is very low.[173] This situation has also been highlighted by Cybercom Group, who are a subcontractor for AWS. Cybercom argues that the reality now is different to when eSam issued their legal statement in 2018. Cybercom points out that certain cloud services are offered from Swedish data centres and that there is are security provisions, such as encryption that the public authority controls entirely on its own in relation to the cloud service provider. The company also argues that detailed knowledge of the technical IT security solution that the cloud service providers offer is needed in order to be able to decide on whether it is unlikely that information will be disclosed in an unauthorised manner. Cybercom's conclusion is that there are no obstacles to municipalities, regions and state public authorities considering using cloud services, even if they are foreign-owned.[174] The company asserts that the same conclusion was reached at a closed roundtable discussion at Almedalen 2019, at which representatives from central Swedish public authorities within data protection

170 The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Preliminary Study Report on Web-based Office Support]*, Ref. 23.2-6283-18, 22-02-2019, p. 35. Note that the Legal, Financial and Administrative Services Agency's position applied only to eSam's statements in 2015 and 2018.

171 Cf ch. 8 § 3 OSL

172 The Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Web-based office support preliminary study report]*, pp. 32–33.

173 See Microsoft, *Molntjänster och säkerhet* 13-12-2018 *[Cloud services and security]*, the Swedish Association of Local Authorities and Regions et al., Open seminar at Almedalen 2019, *CLOUD Act – obstacle or not.*

174 Cybercom also refers to reports from two separate law firms that have analysed the legal situation and concluded that the current regulations give leeway for considering use of foreign-owned cloud services, but that an analysis must take place in each individual case. The company also observes that the people behind eSam's statement in 2018 have now expressed a somewhat milder interpretation of the statement.

and cybersecurity, directors general of state public authorities and representatives of the Swedish Association of Local Authorities and Regions (SALAR) participated.[175]

SALAR, the Swedish Association of Local Authorities and Regions, partly in response to the stance adopted by eSam's in 2018, stated that market-driven cloud services – including those with ownership in a foreign country – are a necessary part of digitalisation. SALAR also observes that a high percentage of Sweden's municipalities and regions already use such cloud services, which in some cases have been procured by state public authorities. Uncertainty with respect to the legal questions is said to have already had the effect of slowing digitalisation and resulted in considerable resources being devoted to interpretation and adaptation instead of reaping the benefits. Since it involves very large - upcoming and already initiated - investments, SALAR has determined that there is a need for a coherent national approach to the matter for public organisations. SALAR has also determined that the lack of a national consensus on the legal situation for cloud services with foreign ownership might lead to major problems for digital collaboration between public stakeholders and ultimately to reduced ability to deliver the services that the general public expects. To the extent that there are limitations on the handling of data, storage or communication of certain sensitive or confidential information as described in the statement by eSam, SALAR argues that this must be clarified by means of supplementary or amended legislation.[176]

EU Data Protection Regulation

When data containing personal information is transferred to a third country (a country outside the EU) in response to a request under the CLOUD Act or similar legislation, this constitutes processing of personal data. The circumstances under which such processing is permitted are regulated by 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), referred to hereinafter as GDPR.

Data Controllers and Data Processors

The data controller is responsible for ensuring that processing of personal data takes place in compliance with GDPR. The data controller is the person who, solely or together with others, determines the purpose and the means of processing personal data. The data controller may appoint a data processor who processes personal data on behalf of the data controller. Such processors are always outside the data controller's organisation and are only permitted to process personal data in line with the instructions of the data controller. The data controller must only appoint data processors who provide adequate guarantees that they will process the information in compliance with the GDPR and that the data subject’s rights will be protected.[177]

When a public authority buys cloud services from a service provider, the public authority becomes the data controller. By concluding a personal data processing

175 Blix Fredrik and Brolin Richard, *Grönt ljus för kommuner, regioner och statliga myndigheter att överväga molntjänster [Green light for municipalities, regions and state authorities to consider cloud services]*, Cybercom Group, 04-07-2019

176 The Swedish Association of Local Authorities and Regions, *Ställningstagande om informationshantering i vissa molntjänster [Position on information management in certain cloud services]*, ref. no. 19/00087, 12-04-2019

177 Articles 4.7, 4.8, 5.2, 26.1, 28.1 and 28.3 in GDPR.

agreement, the service provider is given instructions on the purpose of the processing and how it must take place. The service provider is the data processor as long as they are processing the personal data on the public authority's behalf and in accordance with the agreement. If the service provider were to process the personal data for a purpose other than what is defined in the agreement, the service provider should be considered the data controller.[178] Before a Swedish public authority appoints a service provider as the data processor, however, the public authority must analyse whether this involves a risk that personal information will be processed in a manner that conflicts with the GDPR.

The Relationship between the Cloud Act and the EU Data Protection Regulation

The European Data Protection Board, the European Data Protection Supervisor and the EU Commission have issued statements on the question of whether service providers disclosing personal data stored in the EU to a foreign public authority, for example for law enforcement purposes, is consistent with the GDPR. The European Data Protection Board and the European Data Protection Supervisor suggest a two-stage test to ensure that a transfer of personal data to a third country fulfils the GDPR requirements. Firstly, there must be legal grounds for the processing of personal data and all other requirements in the regulation must be fulfilled, with respect to the general principles on proportionality, accuracy, minimisation of storage, security and so forth.[179] Secondly, the transfer must be in compliance with the provisions in chapter V of the GDPR, which exhaustively regulate the conditions under which personal data may be transferred to a third country.[180]

Legal grounds

A fundamental requirement for a public authority or a company to have the right to process personal data is that there be legal grounds for the processing. The GDPR exhaustively regulates which legal grounds are acceptable. When personal data is transferred to a third country's public authorities after a request in accordance with that country's legislation, there are four main legal grounds that could come into play.

Firstly, the processing may be necessary for compliance with a legal obligation to which the data controller is subject (Article 6.1 c), for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6.1 e). A legal obligation, task of public interest or the exercise of official authority must be laid down by union law or member state law in order to constitute legal grounds.[181] The European Data Protection Board et al. have determined that as long as the procedure in accordance with the CLOUD Act is not recognised by an international agreement between the EU and the USA the legal grounds of legal obligation, task of public interest or exercise of an official authority

178 See article 28.10 in GDPR and the Legal, Financial and Administrative Services Agency, *Förstudierapport Webbaserat kontorsstöd [Web-based office support preliminary study report]*, p. 14.

179 See article 5 of GDPR.

180 See article 44 of GDPR. See also EPDB-EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*,10-07-2019, Annex pp. 3–4

181 See article 6.3 of GDPR. In ch. 2 §§ 1 and 2 of Swedish Act (2018:218) with provisions complementing the EU Data Protection Regulation, there are stipulations that clarify that this requirement from the Swedish side entails that the legal obligation or information in the public interest must be pursuant to law or other legal regulations, collective bargaining agreements or other decisions that have been issued with support of the law or other legal regulations in order to constitute acceptable legal grounds.

cannot apply when a service provider discloses personal data pursuant to a request under the CLOUD Act.[182]

Secondly, the processing may be necessary for purposes that relate to the data controller's or a third party's legitimate interests unless the data subject's interests or fundamental rights and freedoms take precedence and require protection for the personal data (Article 6.1 f). Therefore, a weighing of interests between those of the data controller and those of the data subject must take place. The European Data Protection Board et al. have determined that the data controller's interests could relate to avoiding legal sanctions from the American authorities for failure to obey a request for disclosure. In the absence of an international agreement that supports disclosure pursuant to the CLOUD Act, the European Data Protection Board et al. argue, however, that the transfer would take place without the protection that such an agreement provides for the data subject's right to effective legal recourse (cf Article 47 of the charter). The European Data Protection Board et al. also point out that by its nature a request in accordance with the CLOUD Act makes it practically impossible for the data controller to accurately evaluate all of the circumstances and consequences for the data subject that disclosure might entail. Against this backdrop, the European Data Board et al. have determined that the interests of the data subject in the personal data not being disclosed should outweigh the data controller's interest in disclosing the data in the event that a request for disclosure is made to a service provider in accordance with the CLOUD Act.

Ultimately, the processing may be necessary to protect the vital interests of the data subject or another natural person (Article 6.1 d). According to the GDPR, processing of personal data should only be supported on this legal basis if the processing cannot be manifestly based on another legal basis.[183] Since the processing of personal data which takes place with disclosure of personal data in accordance with the CLOUD Act could instead take place in accordance with the procedure defined in an agreement on mutual legal assistance (MLAT), the European Data Protection Board et al. argue that such a disclosure cannot be considered necessary to protect any natural person's interests other than those of the data subject. The European Data Protection Board et al. do not, however, rule out that a transfer in accordance with the CLOUD Act may be necessary, in exceptional circumstances, to protect the data subject's interests. One example mentioned is when the personal data is needed in an investigation relating to kidnapped children. However, it is noted that such processing must also fulfil the requirements for transfer to a third country as defined in Article 49.1 p (see below).[184]

Transfer of personal data to a third country

The main rule in the GDPR is that a transfer or disclosure of personal data based on a judgement of a court or tribunal or the decision of an administrative authority of a third country may only take place if based on an international agreement between the requesting third country and the European Union or a Member State, e.g. an MLAT (Article 48). As the EU Commission has indicated, it clearly follows from this provision that a court decision from a third country does not in itself means that

182 EPDB-EDPS *Joint Response to the LIBE Committee*, Annex p. 5–6

183 See recital 46 of the GDPR.

184 EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex p. 7–8

a transfer of personal data is legal in accordance with the GDPR.[185] The European Data Protection Board has stated in its guidelines that in situations where there is an MLAT or similar agreement in place, a company within the EU should generally reject direct requests for disclosure and refer the third-country public authority to the existing agreement.[186]

A transfer of personal data may also take place if the Commission has decided that the third country ensures an adequate level of protection. If such a decision has not been made, the personal data may only be transferred to a third country after certain stipulated appropriate safeguards have been provided and on the condition that enforceable data subject rights and effective legal remedies are available to the data subject (Articles 45, 46 and 47). The Commission has taken the position that none of these requirements are fulfilled in a situation where the public authorities in a third country request access to information that is stored within the EU.[187]

Based on the assessments of the European Data Protection Board and the Commission regarding Articles 45-48 of the GDPR, one of the exceptional situations indicated in 49.1 must apply in order for a disclosure of personal data in accordance with a third country's legislation to be legal pursuant to the GDPR.[188] In such situations, there are primarily four derogations that can come into play.

The first derogation pertains to transfers that are necessary for reasons of public interest (Article 49.1 d). The public interest in question must be recognised in EU law or in the national law to which the data controller is subject.[189] The European Data Protection Board et al. argue that consideration cannot be given to a third country's interests in this case. It is also not sufficient that a third country's interests, for example in conducting an investigation, are also, in the abstract sense, in the EU's or a member state's interest.[190]

The other exception that may be applicable is the derogation for transfers that are necessary for the establishment, exercise or defence of legal claims (Article 49.1 e). The European Data Protection Board et al. underscore that this derogation requires a close link between the transfer of data and specific proceedings and that the exception cannot be used to justify transfer of personal data merely because a legal case or formal proceedings may take place in the future.[191]

The third derogation that may come into play is when the transfer is necessary to protect the data subject's or other persons' vital interests when the data subject is physically or legally incapable of giving consent (Article 49.1 f). The European Data Protection Board et al. have determined that, just like the legal grounds in Article 6.1 d, the protection of the data subject's interests could, in exceptional cases, mean that the conditions for this derogation are met. The EDPB et al. have also stated that the

185 *The European Commission, Brief of the European Commission on behalf of the European Union as amicus curiae in support of neither Party in the case United States v. Microsoft Corp.* See also The European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679,* adopted on 25 May 2018 p 5.

186 The European Data Protection Board, *Guidelines 2/2018,* p. 5

187 European Commission, *Brief of the European Commission*

188 If the Commission has not made a decision on an adequate protection level or appropriate protective measures have not been taken, transfer to a third country may only take place if one of the exceptional situations in Article 49.1 of the GDPR applies.

189 See article 49.4 in GDPR.

190 EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex s. 6

191 EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex pp. 6–7 and The European Data Protection Board, *Guidelines 2/2018,* s. 11–12

requirement that the data subject must be prevented from giving their consent may include situations where it is the data subject who constitutes an immediate threat to other persons' lives or physical integrity. However, one stipulated condition is that there should be adequate information to substantiate the legality. The European Data Protection Board emphasises, though, that other persons' interests cannot be used as a legal basis for a transfer to a third country if there are other legal grounds that can be used instead, such as when there is an agreed MLAT procedure.[192]

If none of the aforementioned derogations are applicable, there is a final potential derogation in Article 49.1, paragraph 2 of the GDPR. Under this derogation, a transfer to a third country may only take place if it is necessary for a purpose that relates to the data controller's compelling legitimate interests and the data subject's interests or rights and freedoms do not take priority. Therefore, a weighing of interests must take place with respect to these two opposing interests. The area of application for this exception is particularly narrow and the derogation involves a number of criteria that must be fulfilled in order for it to be applied. The data controller must, for example, have assessed all circumstances surrounding the transfer and provided suitable safeguards for the personal data based on this assessment. The data controller also has an obligation to inform the supervisory authority and the data subject alike.

The EU Commission has indicated that the data controller's interest in not becoming the subject of legal sanctions in a third country would be such a legitimate interest that would fall under this last derogation.[193] E However, the European Data Protection Board et al. have determined that the requirements that must be fulfilled for this derogation are much stricter than those for the application of a weighing of interests as legal grounds in Article 6.1 f of the GDPR. The European Data Protection Board et al. also point out many difficulties in applying this derogation to a request pursuant to the CLOUD Act. Firstly, just as with the weighing of interests as legal grounds, it is difficult to carry out an accurate evaluation of all circumstances and potential consequences for the data subject. Secondly, a request for disclosure pursuant to the CLOUD Act is often associated with a non-disclosure order to avoid putting the criminal investigation at risk. This entails difficulties for the data controller with respect to informing the supervisory authority and the data subject. Thirdly, it is not possible in practice for the data controller to take suitable protective measures for the transfer of data. Against this backdrop, the European Data Protection Board et al. have determined that the exception in Article 49.1 paragraph 2 cannot be applied in order to legally transfer personal data to American authorities after a request pursuant to the CLOUD Act.[194]

The consequence of the conflict between the CLOUD Act and the GDPR for Swedish public authorities

According to the assessment made by the European Data Protection Board et al. there are only legal grounds for a transfer to a third country pursuant to the CLOUD Act in exceptional cases for the purpose of protecting the interests of the data subject. The same applies for the conditions for lawful transfer to a third country in line with the provisions in chapter V of the GDPR.

192 EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex pp. 7

193 European Commission, *Brief of the European Commission*

194 EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex s. 7

A data controller or a data processor who discloses personal data to a third country's authorities without legal grounds for doing so under the GDPR ultimately runs the risk of incurring significant administrative fines.[195] The same applies when personal data is transferred to third countries without any of the conditions in chapter V of the GDPR being fulfilled. A party who fulfils a request in accordance with the CLOUD Act thus risks sanctions pursuant to EU law. Failure to fulfil a request under the CLOUD Act, however, entails the risk of legal sanctions in the USA. In practice, it means that a service provider contracted by a Swedish authority runs the risk of being exposed to a conflict between EU law and American legislation.[196]

A Swedish authority is probably not the data controller for the processing of personal data that takes place when an appointed data processor, such as a service provider, discloses information to a third country in breach of the agreement. As a data controller, however, the public authority can only appoint processors who provide adequate guarantees that the data subject's rights are protected and that the processing takes place in accordance with the GDPR. Deficiencies in such handling of personal data can result in administrative fines.[197] The public authority intending to use cloud service must therefore ensure that they do not contract a service provider who may violate the GDPR or the personal data processor agreement.

195 See articles 44 and 48 compared with article 83.5 c in GDPR. The fines can be as much as EUR 20 million or 4 per cent of a company's global annual turnover.

196 EPDB-EDPS, *Joint Response to the LIBE Committee*, Annex p. 2

197 See articles 28.1 and 83.4 a in GDPR. For a public authority such fines can reach a maximum of EUR 10 million.

Annex 4 Examples of service providers disclosing client data to law enforcement agencies

Many providers regularly publish reports on inquiries from law enforcement authorities relating to data. It is unclear how complete the reports are, and because different organisations publish different information in different ways, they are not comparable. The purpose of this chapter is to provide a general picture based on publicly published information regarding whether data is disclosed by providers and what data is available regarding disclosure by major providers.

Microsoft publishes a report semi-annually. Many of the inquiries relate to the accounts of private persons, but Microsoft also describes inquiries about non-consumer accounts. Microsoft indicated that 61 inquiries were received globally in the second half of 2018 with respect to accounts associated with cloud customers with more than 50 user accounts. Microsoft disclosed data after review in 22 cases. Of those 22 cases, content was disclosed in 15 cases and metadata was disclosed in seven cases. Of the 15 cases where content was disclosed, eight were associated with American law enforcement authorities. During the same period, American law enforcement authorities requested data in 36 cases that related to customers with more than 50 users. Of those requests, one related to data that was stored outside the USA.[198]

AWS does not publish data on private persons' accounts and organisations' services separately. Among other things, AWS publishes the number of requests specifically relating to their AWS cloud service. If inquiries relating to national security that are completely classified are excluded, 271 requests were received in 2018. Data was disclosed in 200 of those cases.[199]

Google continuously publishes reports on requests and disclosure of data to public authorities. They also indicate that they want to be open with the information because they want to bring attention to the large scope of the requests and the laws and legal processes that affect access to information online.

Google also reports the proportion of cases where requests result in disclosure. Google reports that data was disclosed to law enforcement authorities in a total of 375,604 cases in 2011-2018. The number of requests is increasing and data is disclosed in approximately 75 % of the cases.[200]

198 Microsoft, *Law Enforcement Requests Report*

199 AWS, *Information Request Report*

200 Google, *Request for user information*

Annex 5 Protective Security

The provisions on protective security are an important part of the protection of sustaining societal functions. This annex provides a brief overview of the protection for security-sensitive activities stipulated in the Swedish Security Act (2018:585).

Security-sensitive activities, information security and personnel security

The Swedish Security Act applies to parties conducting security-sensitive activities, which include activities that are of importance to Sweden's security.[201] The party conducting security-sensitive activities must take preventative action to protect said activities from espionage, sabotage, acts of terror and certain other threats.[202] Security-sensitive activities are identified based on the damage that will be caused to Sweden's security if an attacker obtains information about the activity, destroys information or impairs the function of the activity in some other way.[203] The protective security must be provided based on a protective security analysis for the purpose of identifying which activities and what information are covered by the Swedish Protective Security Act and whether the protection thereof is adequate.[204] The requirements on the handling of classified information increase along with the classification level.

Security-sensitive activities are conducted by Swedish public authorities, such as the Swedish Social Insurance Agency. The Swedish Protective Security Act contains provisions on what protective security measures must be taken for security-sensitive activities. These measures include information security and personnel security.[205]

Information security involves protecting information, regardless of where it is located, in a manner such that it cannot be shared with or changed by unauthorised persons. It also involves ensuring that data is available when it is needed. This is all for the purpose of avoiding the negative consequences for an activity that such situations might entail.[206]

An employee or other participant in a security-sensitive activity is normally assigned a security class based on what type of information the person will encounter and the extent to which that will take place.[207] When employed by the state, municipality or regional authority with security class 1 or 2, Swedish citizenship is a requirement. However, this requirement does not apply to other participation in security-sensitive activities that are conducted for the state, municipality or regional authority.[208] The purpose of personnel security is to prevent persons who are not trustworthy from a

201 ch. 1 § 1 Swedish Protective Security Act.

202 ch. 1 § 2 Swedish Protective Security Act.

203 ch. 2 § 5 Swedish Protective Security Act. The four security classifications are 1) classified (top secret), if the damage that can occur is exceptionally grave, 2) secret, causing serious damage, 3) confidential, causing damage that is not insignificant and 4) restricted secrecy, causing only minor damage.

204 ch. 2 § 1 Swedish Protective Security Act.

205 Physical security is also included. See Chapter 2 §§ 2-4 Swedish Protective Security Act.

206 ch. 2 § 2 Swedish Protective Security Act. See also the Swedish Security Service, *Informationssäkerhet [Information security]*.

207 ch. 3 §§ 5–10 Swedish Protective Security Act

208 ch. 3 11 § Swedish Protective Security Act

security perspective from participating in an activity where they may gain access to classified information or from participating in an activity that is security-sensitive for some other reason. Personnel security must also ensure that the persons who participate in security-sensitive activities have adequate knowledge about protective security. The party who employs or contracts a person in a security-sensitive activity must conduct a background check before the person participates in the activity. This applies regardless of whether the participation will take place through employment or in another manner. The purpose of the check is to determine whether the person can be assumed to be loyal with respect to the interests that must be protected and that the person is otherwise trustworthy from a security standpoint. Another purpose is to investigate potential vulnerabilities that could result in the person finding themselves in an exposed situation and being vulnerable to external pressure.[209]

A background check on persons who will participate in security-sensitive activities must be carried out by the party deciding on the employment or other form of participation in the security-sensitive activity. If a public authority has the decisive say over the concerned person's suitability to participate in a security-sensitive activity conducted by an individual organisation, it is the public authority that must make the ultimate decision.[210] The security check normally consists of a basic assessment, check of registers and training in preventive security. The basic assessment contains a review of the person's personal circumstances insofar as they may be significant to the background check. This will include a background check interview, which is one of the key tools to provide a basis for this assessment. In addition, relevant certificates, grades and references may also be collected and evaluated. Other information from open sources, social media and the internet, etc. can also contribute to provide a more complete picture of the person.[211] After a basic assessment with satisfactory results with respect to loyalty, trustworthiness and vulnerability, the background check is normally supplemented with a register check by the Swedish Security Service if the position is security classified.[212] The register check includes information that is collected from criminal records, "suspicion directory" and information that is processed with the support of the Swedish law (2018:1693) on processing of personal data by the police within the sphere of the Criminal Data Act.[213]

With respect to persons who have resided in another country, however, the Swedish Security Agency has limited possibilities of conducting qualitative register checks. The Swedish Security Service stresses that this must be taken into account by the organisation responsible for the activity by means of a more thorough background check, etc. According to the Swedish Security Service, higher demands should be placed on collection of references for background checks on persons who have not resided in Sweden, because the possibilities for utilising Swedish means of investigation are limited in foreign countries.[214]

209 ch. 2 § 4 and ch. 3 §§ 1–2 Swedish Protective Security Act See also the Swedish Security Service, Personnel security.

210 ch. 3 § 4 second paragraph Swedish Protective Security Act and ch. 5 § 4 Swedish Protective Security Ordinance. See also Swedish Security Service, *Guidelines for protective security – personnel security*, June 2019 p. 18

211 ch. 3 §§ 3 and 4 Swedish Protective Security Act (2018:585), ch. 5 § 2 Swedish Protective Security Ordinance. (2018:658) and ch. 6 § 4 the Swedish Security Service's regulations (PMFS 2019:2) on protective security See also the Swedish Security Service, *Vägledning i säkerhetsskydd [Guidelines for protective security]*, p. 11–12

212 ch. 3 § 14 Swedish Protective Security Act (2018:585)

213 ch. 3 § 13 Swedish Protective Security Act

214 Swedish Security Service, *Vägledning i säkerhetsskydd [Guidelines for protective security]*, p. 26

Protective security in procurement

Security-sensitive activities must have the same protection regardless of who carries out the activity. A public authority must, therefore, require the same level of security protection from providers as they require in their own organisation.[215] Protective security in procurement is the process by which the procuring public authority analyses the security values that are involved in the procurement process. State authorities, municipalities and county administrative boards responsible for certain types of procurement processes associated with security-sensitive activities must conclude a security agreement with the tendering party or provider specifying how they must fulfil requirements on protective security. Such agreements must also be signed with any subcontractors. The authority must also check and follow up to ensure that the providers have actually taken the measures that the authority requires.[216] One of the risks involved with procurement in connection with security-sensitive activities is, according to the Swedish Security Service, that the demands specified in the protective security agreement are sometimes so generally defined that they are difficult to monitor.[217]

The protective security agreement also constitutes a basis for deciding which employees and other participants from the provider should be assigned a security classification. When a public authority signs a protective security agreement with a provider, it must be reported to the Swedish Security Service. The purpose of doing so is for the Swedish Security Service to conduct a register check on people who will have classified roles in connection with the agreement.[218]

215 The Swedish Security Service, *Säkerhetsskydd vid upphandlingar och affärsavtal [Protective security for public procurement and commercial agreements]*

216 Ch. 2 § 6 Swedish Protective Security Act. The decision relates to procurements and agreements relating to goods or construction contracts if there is information on the subject of procurement that is security classified as confidential or higher, or if the procurement otherwise relates to or gives the provider access to a security-sensitive activity of importance to the security of Sweden.

217 Swedish Security Service, *Årsbok [Annual Report]* 2017, p. 56

218 The Swedish Security Service, *Säkerhetsskydd vid upphandlingar och affärsavtal [Protective security for public procurement and commercial agreements]*

Annex 6 Classification of vital societal functions – the Swedish Transport Agency as an example

The Swedish Transport Agency works to achieve good accessibility, high quality and safe and environmentally-compatible transportation by rail, air, water and road. The Swedish Transport Agency drafts regulations, issues permits and monitors these for compliance. Using registers, the agency works with fines, permits and changes of ownership.

In 2017 the Swedish Transport Agency conducted a security analysis in order to identify activities in need of protection, potential antagonists, consequences of disclosure or destruction and measures to eliminate vulnerabilities. The security analysis is not publicly available, but certain general conclusions have been published in a study requested by the government.[219]

According to the security analysis the Swedish Transport Agency handles large amounts of information and data. A very small part of the information is considered confidential. However, the majority of the information should be considered public and can be requested by the general public.

Another problem is that the overall volume of information in and of itself is an asset worth protecting. That is because it involves very detailed basic data with extensive details that provide a comprehensive picture of the information content from various security perspectives. A party having access to the entire set of data can analyse the information to find discrepancies and thereby draw conclusions to access confidential information. With unlimited access to large amounts of information, there are also risks of measures and analyses that should not take place for security reasons. A lack of information that should be available can also constitute a risk.[220]

In the assessment of the Swedish Transport Agency's outsourcing in 2017, it was determined that for security reasons the Swedish Transport Agency's strategy would be to minimise the number of people who had knowledge of what type of information the agency handled. The information volume as a whole should thus be considered security-sensitive. Since the data subject to secrecy and confidentiality is dispersed throughout the rest of the information, it becomes problematic to design IT support where certain areas should be considered vital societal data while other parts are not.[221]

219 The Swedish Transport Agency, *Kartläggning av hanteringen av vissa uppgifter [Survey of the handling of certain data*

220 For example the Swedish Police Authority conducts checks against the Swedish Transport Agency's register when required.

221 SOU 2018:6, *Granskning av Transportstyrelsens upphandling av it-drift, [Study of the Swedish Transport Agency's procurement of IT services*, p. 76–77, 84, 100, 220 and 223

Annex 7 Encryption to limit disclosure of data

Encrypting means that data is made difficult to read for anyone who should not read it. To make the data readable again, decryption is necessary. It means that the party decrypting the information and the party who should read the information must have access to the key that is needed to decrypt the information. Not least, military and political organisations have extensive experience with encryption. The purpose of encryption is to prevent unauthorised parties from gaining access to data.

As long as encryption has existed, however, unauthorised parties been attempting to obtain encryption codes in order to gain access to data.

With the introduction of computers, encryption and decryption have been automated and encryptions must be increasingly complex so that they cannot be broken by unauthorised persons.

Encryption can essentially be suitable in two principle situations: when data is stored and when it is transported. Since the challenges are different for storage and transport, it is important to be able to ensure which type of encryption is applicable.

However, it is also important to consider that basically data cannot be processed when it is encrypted. In order to be able to process data, it must first be decrypted. This means that if processing is carried out by a provider, the provider must have the possibility of decrypting.

Under ch. 3 § 5 of the Protective Security Ordinance (2018:658), all activities and functions, public and private, involving classified information that is to be communicated to an information system outside the activity operator's control must protect the information using cryptographic functions that have been approved by the Swedish Armed Force [222]. The Swedish Armed Forces cryptographic functions are not intended for or suitable for all types of information and activities.

Providers can offer their customers encryption as part of a service provided. The services and protection that are offered vary and should only be considered here as an example. However, it is worth noting that many of the services that are offered by the major cloud service providers are not approved by the Swedish Armed Forces.

Microsoft offer three basic services for encryption in their cloud services: Customer key, Bring your own key and Hold your own Key. AWS also offers encryption services where both the customer and AWS hold the key and the example below illustrates just one example of such an application.[223]

222 The Swedish Armed Forces, *Försvarsmaktens föreskrifter om signalskyddstjänsten och Försvarsmakten, Godkända kryptoapparater, September 2019 [The Swedish Armed Forces regulations on the signal protection service and the Swedish Armed Forces, Approved cryptography devices]*

223 AWS, *Protection Data using encryption*

Customer key/service encryption

Microsoft offers this service for Sharepoint Online, Onedrive Business and Exchange Online. The service entails protection against physical access to data if, for example, an unauthorised party gains access to a hard drive.

The encryption method does not protect against access to data by authorised persons. Data encrypted using this method can be accessed by the provider's authorised technicians and can be disclosed to a foreign public authority under applicable legal regulations.[224]

Bring your own key

Microsoft offers this service for encryption of individual documents and it can thus be suitable for individual email messages or documents.

The owner can choose to encrypt the document. However, Microsoft has access to the key in order to be able to read and index data and protect documents from unauthorised access.

Data encrypted using this method can be made available by the provider's authorised technicians and can be disclosed to a foreign public authority under applicable legal regulations.[225]

Hold your own key

This service is offered by Microsoft for encryption of individual documents and can thus be suitable for individual email messages or documents. The owner can choose to encrypt the document. However, the customer owns the entire chain of keys, which means that the provider does not have access to keys for decryption.

This lack of access means, however, that the usability of the IT services becomes very limited. An example is that the user cannot use search functions and cooperation with other external parties becomes very limited.

This method would, assuming that a foreign public authority did not demand access to the encryption key, prevent access by the provider's authorised technicians and data could not be disclosed in a decrypted form to foreign public authorities under relevant legal regulations.

This solution would, however, entail diminished functionality for the users in everyday use of office programs, etc. This is partly because certain functions would not be available at all and partly because performance would be negatively influenced.[226]

[224] Microsoft, *Service encryption with Customer Key for Office 365 FAQ FAQ*

[225] Microsoft, *Price levels and restrictions for BYOK*

[226] Microsoft, *Hold your own key protection (HYOK) for Azure Information Protection*

Foreign public authorities' access to encryption keys

Laws on transfer of encryption keys are in existence in a number of countries. The Council of Europe proposed in 2013 that this possibility should be introduced within the EU.[227] Such legislation is not currently in place in Sweden. However, on 24 October 2019, the government decided in favour of the proposal on legislation for Secret data surveillance. It was proposed that law enforcement authorities should be given the possibility of using decryption as a secret means of coercion where there is suspicion of serious crime.[228]

Denmark was the first country in Scandinavia to introduce legislation that allowed secret data surveillance in 2002. Since then, equivalent legislation has also been introduced in Finland and Norway and the legislation includes the possibility of decryption.[229]

A study that was commissioned by the EU Parliament in 2017 found that methods for secret data surveillance are used in the EU States that were compared, in some cases, with explicit support of the law and in others without. In the states where there is no explicit legislation, legislation is currently being drafted.[230]

Three non-European countries were also analysed in the European Parliament's assessment. It was found that Australia lacked explicit legislation, but the assessment could not rule out the possibility of secret means of coercion being used on the basis of different, older legislation.[231] It was found that Israel has clearer legal latitude and sometime provides leeway for decryption.[232]

Since the example that is used here describes American legislation, the current legal status in the USA is also used to exemplify foreign authorities' possibilities of gaining access to encryption keys in greater detail. The assessment that was commissioned in 2017 by the European Parliament also highlighted how secret means of coercion are used by American law enforcement authorities.[233]

The Fifth Amendment of the U.S. Constitution stipulates that a person cannot be forced to furnish evidence that would work against their own case and thus might be seen as an obstacle to demanding access to encryption keys.[234] However, there are legal cases where encryption keys and passwords have been handed over. The first case was *In re Boucher*, where the accused had initially promised access to their hard drive, but parts of the hard drive were encrypted and not all information was made accessible. The prosecutor asserted that they did not demand that the accused provide the password, rather that the content should be made available to the grand jury and that it would thus not be in violation of the Fifth Amendment of the Constitution and

227 Study of the IT crime convention, *The Council of Europe Convention on IT-Related Crime* (SOU 2013:39), p. 280 et seq

228 The Ministry of Justice, proposal referred to the Council on Legislation for consideration *Hemlig dataavlyssning [Secret data surveillance]*, 24-10-2019, pp. 1 and 57

229 Utredningen om hemlig dataavläsning [Investigation on secret data surveillance], *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet, [Secret data surveillance - an important tool in the fight against serious crime]* (SOU 2017:89), p. 121–147

230 European Parliament, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, (PE 583.137), pp. 72–110

231 PE 583.137 pp. 111–116

232 PE 583.137 pp. 117–120

233 PE 583.137 pp. 121–128

234 Corey Varma, *Encryption vs. Fifth Amendment*

the judge approved this request, because the accused had already offered to provide access to the hard drive.[235]

In another legal case, it was deemed that the Fifth Amendment was applicable and encryption keys were not handed over. In this case, the American FBI seized a number of computers and hard drives, but was unable to decrypt the hard drives. The Electronic Frontier Foundation (EFF) took up the case and the 11th U.S. Circuit Court supported the EFF's request and asserted that the man's encryption keys were protected by the Fifth Amendment.[236]

The request for encryption keys via a provider was covered in a report from Massachusetts Institute of Technology (MIT). The report describes how there was already a proposal in 1997, Clipper Chip, that required that all powerful encryption systems would be located on the premises of a trusted party and could be disclosed to law enforcement authorities after a legal action. The costs and risks were ultimately deemed to be too great and the project was abandoned.[237]

The report analysed the 2015 proposals submitted to provide American law enforcement authorities the possibility of gaining access to encryption keys after conclusion of a lawsuit. The report asserts that this would have the consequence that the functions that are now being introduced in order to make the internet more secure would probably have more limited distribution, because faith in the protection would be damaged. The report also stresses that if providers were obliged to be able to supply encryption keys, it would in practice lead to more complex systems that would give rise to new risks. Ultimately, it was determined that functions for the ability to decrypt become a target themselves for antagonists, which can result in further vulnerabilities.[238]

Taken as a whole, the legal situation for American public authorities' possibilities of gaining access to encryption keys after a lawsuit is unclear and depends on the evaluation in each individual case.

What the legal situation would be when a provider is located in one country but data is stored physically in a different country seems unclear, particularly since the regulations can vary depending on potential agreements between countries and a service can consist of services from different providers from different countries. If a provider or a service is purchased, the legal situation becomes even more difficult to evaluate.

235 United States District Court for the District of Vermont. No. 2:06-mj-91, 2009 WL 424718 Feb. 19, 2009. *Memorandum Of Decision In re Grand Jury Subpoena to Sebastien Boucher*

236 EFF in the United States Court of Appeals for the Eleventh Circuit *Case: 11-12268*

237 Abelson Harold et al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications 2015* (MIT-CSAIL-TR-2015-026) p. 6.

238 Abelson Harold et al. *Keys Under Doormat* p. 24 et seq

Annex 8 Management of telemetry data by service providers

Telemetry data is measurement data. Many providers collect telemetry data and the examples below serve only as an illustration.[239]

According to Microsoft, the company uses telemetry data to

- keep an application updated,
- ensure that an application is secure, reliable and works well,
- improve an application because Microsoft can analyse aggregated user data,
- personalize the user experience and
- create an understanding of how the users use and do not use functions.[240]

Microsoft has indicated that they collect the following telemetry data relating to Windows.

- type of hardware,
- which applications are installed on the unit and how they are used,
- how well drive processes work and
- the user's settings.

In 2017 the Dutch Data Protection Authority analysed telemetry data in Windows 10.[241] The investigation shows that even if the user chose the most limiting settings, sensitive data was sent to Microsoft. With use of the most permissible settings, very sensitive data, such as websites visited and contents in document, was sent. The study showed that data that was collected from use of application included sensitive personal data, such as that from an application for Muslim prayer times and an application for pregnant women. One use of the data that was collected was to present personalised advertisements to users.[242]

In 2018 the Dutch government commissioned a consequence evaluation in accordance with the GDPR that covered telemetry data in Microsoft Office Pro Plus, including standalone Office 2016 and Office 365. The purpose was to help state organs survey and assess the risks in relation to the data subject with such use and to plan adequate measures to manage them.[243]

239 Telemetry data is collected not only from users of public cloud services but, as the example shows, telemetry data can also be collected from services that are installed on the customer's equipment. However, public cloud-based services provide greater opportunity for collection of telemetry data.

240 Microsoft, *Configuring diagnostic data for Windows in your organisation*, 2019

241 Autoriteit Persoonsgegevens (Dutch DPA), *Summary of Investigation Report Public Version Microsoft Windows 10 Home and Pro*, August 2017. Note that Windows 10 is not a public cloud service.

242 The report does not explicitly describe how data is managed and which third parties have gained access to it, but it cannot be ruled out that data has been made accessible to third parties in order to enable personalised advertisements.

243 Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data*

According to the consequence evaluation, Microsoft, for example, collects an estimated 25,000 different type of events on Office 365. Telemetry data is sent encrypted to Microsoft's servers. Microsoft also collects telemetry data relating to the Windows 10 operating system, but that is limited to 1,000 events. According to the answers provided by Microsoft during the investigation, a number of development teams have global access to data.

The investigation with respect to Office Pro Plus identifies the following risks with Microsoft's access to this data.

- There is insufficient transparency for the general public regarding which information Microsoft receives, because there is no publicly available information. This prevents an organisation from conducting a risk assessment.
- There are no means of controlling which telemetry data is sent.
- Microsoft collects and stores potentially sensitive data in the form of metadata[244] and content[245], for which there is no support under law.
- Microsoft functions as data processor instead of joint data controller, which they should do according to Article 26 of the GDPR.
- There is inadequate control over subprocesses and actual management.
- There is inadequate restriction of the purposes for which data is collected and new events are added for updates, etc.
- Transfer takes place to countries outside the EU.
- It is unclear how long data is stored and there is not adequate opportunity for customers to remove data.[246]

The Dutch government negotiated a supplemental agreement with Microsoft in 2019 that modified the terms for Microsoft Office Pro Plus so that they were consistent with GDPR.[247] The supplemental agreement regulates the specific situations in which Microsoft is permitted to collect telemetry data and how data must be anonymised. It also means that Microsoft is prohibited from using customer data for profiling and advertisement and the like, and that there is the opportunity for the customer to disable the possibility of data collection. The agreement also includes provisions on the opportunity for the customer to call for an audit by an external party in order to ensure that Microsoft is handling data in accordance with the agreement. The Dutch government has the ambition of making the supplemental agreement available for the entire public sector within the EU.[248]

244 For example, if a user clicks the back button several times in a row and the IP number.

245 For example, the message title is collected.

246 Ministry of Justice and Security Strategic Vendor Management Microsoft, *DPIA Office 365 ProPlus version 1905 (June 2019) Data protection impact assessment on the processing of diagnostic data* p. 76 et seq.

247 The agreement was negotiated by a public authority under the government, Microsoft Strategic Vendor Management Office (SLM Rijk). The agreement applies to Microsoft Office Pro Plus and the mobile applications and does not cover Microsoft Office 365.

248 See Strategic Vendor Management Microsoft for the Dutch Government and Ministerie van Veiligheid en Justitie, *EU Software and Cloud Supplier Customer Council* and Ministerie van Justitie en Veiligheid *Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft (Ons kenmerk 2635551)* 01-07-2019.

The Swedish Social Insurance Agency's increasing dependency on secure, user-friendly and robust digital services requires the agency to determine if and when it is appropriate and feasible to use public cloud services that are offered by private suppliers.

The analysis in this white paper is based on the activities of the Swedish Social Insurance Agency. However, it is our hope that it can be used as an aid for other public authorities looking to develop a digital strategy for their sustaining societal functions.