LEXOLOGY

Cloud computing in Sweden

Advokatfirman Delphi

Sweden | March 21 2019

Use the Lexology Getting the Deal Through tool to compare the answers in this article with those from other jurisdictions.

Market overview

Kinds of transaction

What kinds of cloud computing transactions take place in your jurisdiction?

The demand for and use of cloud-based services in Sweden is rapidly growing. There is also an increased focus on information security due to additional requirements in this respect when processing critical or sensitive information. The services and cloud infrastructure varies depending on the users' requirements and needs. There are three internationally established types of cloud services that describe three different function areas: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS). All three are used on the Swedish cloud service market to various extents.

In a recent study carried out by the Swedish Pension Agency determining the most used services among public authorities in Sweden, the Agency concluded that IaaS was used by 30 per cent, PaaS by 23 per cent and SaaS by 78 per cent. This may lead to a conclusion that SaaS is the most common cloud service used by Swedish authorities (source: Pensionsmyndigheten - Molntjänster i staten - En ny generation av outsourcing).

Another report from 2016 that examined the private sector's use of cloud services presents similar conclusions. Out of the top 200 Swedish public cloud computing providers, SaaS constitutes 76 per cent of the segment, while IaaS represents 22 per cent and PaaS only 2 per cent. Out of the SaaS providers, 62 per cent use IaaS partners, out of which half of the infrastructure providers are located in Sweden. The remaining SaaS providers have their own infrastructure. Recently, Sweden has also seen an increase in the number of SaaS providers owing to an uptake in the number of e-commerce services, fintech development and general digitalisation (source: METISfiles - Cloudscape Sweden V1.1, September 2016).

When looking at the different models for providing cloud services in Sweden, the NIST and ISO standard describe four ways of service deployment: public clouds, partner clouds, hybrid clouds and private clouds. Hybrid clouds are quite common within both the public and private sector, and reports are stating that the use will probably increase in the future. Among public authorities, partner clouds are often used to ensure that all security requirements are met, which has been a concern in the use of public clouds (source: Pensionsmyndigheten - Molntjänster i staten - En ny generation av outsourcing).

Recently, Sweden has had numerous notable cloud transactions and has been described as a leading country when it comes to innovation and risk capital investment. Just a few years ago, Amazon moved part of its cloud service, Amazon Web Service (AWS), to Sweden and is currently planning the move of its e-commerce as well.

Active global providers

Who are the global international cloud providers active in your jurisdiction?

Sweden is an attractive market for cloud providers and many of the international providers are active within Sweden. Many Swedish SaaS providers prefer to use a Swedish IaaS partner; however, the largest hosting partner within Sweden is Amazon (US) that represents 32 per cent of the segment, followed by Microsoft, Hetzner and Rackspace. Other international cloud providers active in Sweden are giants such as Google, Dropbox, LinkedIn, Facebook and iCloud; however, this is not a conclusive list (source: METISfiles - Cloudscape Sweden V1.1, September 2016).

Active local providers

Name the local cloud providers established and active in your jurisdiction. What cloud services do they provide?

There are numerous Swedish cloud service providers. Important local IaaS providers are, inter alia, Zitcom, TDC Hosting, Loopia, Bahnhof and Glesys. These providers are common hosting partners to SaaS providers. Among the top Swedish SaaS providers are iZettle and Klarna (payment), Truecaller and Tele2 (communications), and Ericsson. There are fewer Swedish PaaS providers. However, local PaaS providers that can be mentioned are Accedo, Bariumlive and Cloudnet (source: METISfiles - Cloudscape Sweden V1.1, September 2016).

Market size

How well established is cloud computing? What is the size of the cloud computing market in your jurisdiction?

The cloud adaption in Sweden is among the largest in Europe - in 2016, almost 48 per cent of Swedish enterprises used cloud computing services. Only Finland had a higher share of enterprises using cloud computing services in the European Union (source: Eurostat - Cloud computing: statistics on the use by enterprises, December 2016). The total cloud computing market in Sweden was valued to 16 billion krona in 2016 and the annual growth is currently estimated to be around 30 per cent (source: Framtidens Karriär - Kostnadsjakt driver molntillväxt, 2017-02-07).

Impact studies

Are data and studies on the impact of cloud computing in your jurisdiction publicly available?

There are some reports published regarding cloud computing in Sweden. A notable report on cloud computing's impact on state agencies was published by the Swedish Pensions Agency in January 2016. The Swedish Pensions Agency concluded in its report that factors such as innovation, cost-efficiency, flexibility and accessibility are strongly benefited by the use of cloud services. Furthermore, the report concludes that cloud services could have a positive effect on the cooperation between authorities and simplify the access to governmental data and services (source: Molntjänster i staten - En ny generation av outsourcing, Pensionsmyndigheten, January 2016).

The Swedish Civil Contingencies Agency and the Swedish Data Protection Authority (DPA) have published guidelines and policies for public authorities regarding, inter alia, information security requirements in the public procurement process for cloud services as well as privacy concerns that must be considered.

In addition, the Swedish government has taken further steps to ensure continued digital growth. In 2016, it presented five strategic cooperation programme that will help meet several of the social challenges facing Sweden. To stimulate digitalisation of Swedish industry, the Swedish government is requesting extensive cooperation between different actors (source: Regeringen - Strategiska samverkansprogram en kraftsamling för nya sätt att möta samhällsutmaningar).

The research company METISfiles has published its report Cloudscape 2016: An Overview of the Swedish and Danish Cloud Market in English that examines the cloud market in these countries.

Policy

Encouragement of cloud computing

Does government policy encourage the development of your jurisdiction as a cloud computing centre for the domestic market or to provide cloud services to foreign customers?

Sweden is currently attracting foreign risk capital investors due to the fast digitalisation and innovation. Numerous governmental initiatives have been launched to ensure that Sweden continues to develop in the digital arena and to live up to future requirements regarding privacy, IT and security. As one step in this process, the Swedish government requested the Swedish Pension Agency to analyse and evaluate the potential for using cloud services within the public sector and by the state in a way that contributes to a simpler, more transparent and efficient management. Other steps consist of a strong focus on general digitalisation both within the administration and the private sector.

Incentives

Are there fiscal or customs incentives, development grants or other government incentives to promote cloud computing operations in your jurisdiction?

Various grants are available for small to medium-sized companies for projects involving innovation and digitalisation and are awarded by the Swedish government, public agencies and other organisations. Support to large companies also occurs, one significant example being the regional investment grant of around 100 million kronor awarded by the Swedish Agency for Economic and Regional Growth when Facebook established server halls in Luleå in the north of Sweden in 2011. Grants also exist for the expansion of the Swedish IT infrastructure.

Legislation and regulation

Recognition of concept

Is cloud computing specifically recognised and provided for in your legal system? If so, how?

There is no specific recognition of cloud services in Swedish legislation.

Governing legislation

Does legislation or regulation directly and specifically prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

As a general rule, Sweden lacks direct and specific regulation regarding cloud computing as such. Swedish legislations and regulations are in general technology neutral, which implicates that Swedish legislations lacks that sort of specific targeting. However, the legal concerns are regulated indirectly in several legislations and regulations. The most relevant regulations are MSBFS 2016:1 and MSBFS 2016:2 that regulate the public authorities' internal information security policies and work, as well as the requirement to report IT incidents to the Swedish Civil Contingencies Agency. Cloud services are regulated by explicit requirements for internal policies and routines regarding incident management, the requirement that organisations must be able to handle threats and risks through models and routines for incident and continuity management.

Sweden has implemented the NIS Directive (EU) 2016/1148 through the Act on Information security for vital societal functions and digital services (SFS 2018:1174), thereby extending the requirements on security and to report IT incidents to cloud service providers.

What legislation or regulation may indirectly prohibit, restrict or otherwise govern cloud computing, in or outside your jurisdiction?

Regarding indirect regulations and legislation, there are several to take into account. When using cloud services to store data from telecoms or e-commerce business, it is important to observe the Electronic Communications Act (SFS 2003:389), which aims to provide individuals and authorities with secure and effective electronic communications, and the Electronic Commerce Act (SFS 2002:562), which states an obligation to provide certain information to customers.

However, the main legislation to take into account regarding cloud services are the provisions on privacy and information security. On 25 May 2018, the General Data Protection Regulation (GDPR) entered into force in Sweden and provides significantly stricter standards, for example, on impact assessments and information security.

Information security is regulated throughout different provisions, such as regulations from the Swedish Civil Contingencies Agency, the GDPR and sector-specific regulations, such as within the healthcare sector. Swedish public authorities are subject to the principle of public access to public documents, which means that all documents submitted to or drawn up by the authority are, in principle, public documents and must be made available for anyone to read. Exemptions from this rule are documents that are subject to statutory secrecy under the Public Access to Information and Secrecy Act (SFS 2009:400) (the Secrecy Act), which means that they may not be disclosed to any third party. In cases where such classified information will be processed in the cloud, additional restrictions regarding the data apply and must, inter alia, be taken into consideration when assessing the risks and which security measures must be implemented.

In addition, if information subject to secrecy under the Secrecy Act may be available to the provider as a result of an agreement between the parties, it must be evaluated whether the data becomes ‘disclosed’ within the meaning of the Secrecy Act. Thus, one opinion is that the Secrecy Act generally prevents authorities from using cloud services. Another opinion is, however, that it is possible for authorities to use cloud services if the relevant authority has made a thorough assessment of the risks based on the character of the information, but further clarification on how these rules are to be interpreted is needed.

Furthermore, public authorities must also comply with numerous other pieces of legislation such as the Archives Act (SFS 1990:782), the Administrate Procedure Act (SFS 1971:291), the Public Procurement Act (SFS 2016:1145) and the Security Protection Act (SFS 1996:627). Also, many public authorities and agencies have sector-specific provisions regarding data processing and information security requirements such as the Patient Data Act (SFS 2008:355).

Breach of laws

What are the consequences for breach of the laws directly or indirectly prohibiting, restricting or otherwise governing cloud computing?

The failure to report an IT incident under the Act on Information security for vital societal functions and digital services is subject to administrative fines. Further, the rules indirectly regulating cloud computing in Sweden are connected to several sanctions and consequences for breaches thereof. The sanctions for lack of compliance with the GDPR include prohibitory injunctions, payment of damages as well as administrative fines. Lack of compliance with the Electronic Communications Act (SFS 2003:389) and the Electronic Commerce Act (SFS 2002:562) may also cause sanctions, such as prohibitions and orders combined with penalties as well as damages

and criminal proceedings. Breaches of the Secrecy Act (SFS 2009:400) may lead to disciplinary or criminal proceedings. There are also various sanctions of similar character for the sector-specific regulation as well as supervision from relevant public agencies.

Consumer protection measures

What consumer protection measures apply to cloud computing in your jurisdiction?

There is no cloud service-specific regulation protecting the rights of consumers in Swedish law, but the Swedish consumer protection legislation includes legislation with focus on e-commerce and digital transactions including Distance and Off-Premises Contracts Act (SFS 2005:59), Consumer Contracts Act (SFS 1994:1512) and the Electronic Commerce Act (SFS 2002:562). The standard Swedish consumer protection for buying goods and services, the Consumer Sales Act (SFS 1990:932) and the Consumer Services Act (SFS 1985:716), is not directly applicable on purchases of digital content, but is still considered to have an impact when courts are evaluating consumer contracts. The consumer protection legislation, inter alia, ensures the consumer rights in regards to quality and performance from the commercial actor, includes the right to withdraw from distance and off-premises contracts within 14 days, bestows a responsibility for commercial actors to provide consumers with information, and provides that courts can prohibit contract terms that are unfair towards consumers from further use and may interpret vague contract terms in favour of consumers. The Swedish consumer protection for digital services is also continuously affected by the EU digital single market reform, and now includes the right to settle disputes online through the Alternative Dispute Resolution For Consumer Disputes Act (SFS 2015:671), and principles about net neutrality and open internet access through Regulation (EU) 2015/2120, as well as a new proposed directive regarding contracts for the supply of digital content.

Sector-specific legislation

Describe any sector-specific legislation or regulation that applies to cloud computing transactions in your jurisdiction.

There is a wide variety of sector-specific legislation in Sweden that concern both private and public actors. There is no legislation that covers cloud computing in particular but these services often fall within the scope of the legislation depending on the sector of operation. Some significant legislation concerns matters of national security in the Security Protection Act (SFS 1996:627), with specific requirements of, for instance, information security and access to information. A new, more stringent Security Protection Act (SFS 2018:585) has been enacted and will enter into force on 1 April 2019.

Cloud companies competing in providing services for public institutions are covered by the Swedish legislation on public procurement - inter alia, the Public Procurement Act (SFS 2016:1145). Public agencies are encouraged by the Swedish Civil Contingencies Agency to use private or partner clouds to be able to provide the necessary security.

There is specific regulation for the processing of personal data in, among others, the health and finance sectors of relevance for transactions in these sectors. In the health sector, personal data is governed by the GDPR supplemented by the Patient Data Act (SFS 2008:355). The legislation in the finance sector, most significantly the Banking and Finance Business Act (SFS 2004:297), is complemented by regulations from the Financial Supervisory Authority, including, inter alia, rules regarding outsourcing and information security.

Other sector-specific legislation that is worth noting includes the energy and telecommunications sectors. For private actors, there are no sector-specific requirements regarding cloud service infrastructure besides the above-mentioned requirements in the Act on Information security for vital societal functions and digital services and careful assessments regarding privacy and IT security.

Insolvency laws

Outline the insolvency laws that apply generally or specifically in relation to cloud computing.

There is no specific insolvency legislation that applies to cloud computing in Sweden, but the standard legal framework for insolvency apply, notably the Bankruptcy Act (SFS 1987:672), the Enforcement Code (SFS 1981:774) and general Swedish principles of property law. For movable property, the right to property is, in general, decided by who is in possession of the property. For intellectual property, the right to the property is instead decided from what is stipulated by contract.

Data protection/privacy legislation and regulation

Principal applicable legislation

Identify the principal data protection or privacy legislation applicable to cloud computing in your jurisdiction.

Since 25 May 2018, the GDPR is the principal legislation governing data protection in relation to cloud computing in Sweden. The GDPR is supplemented by the Data Protection Act (SFS 2018:218) and various sector-specific legislation.

Cloud computing contracts

Types of contract

What forms of cloud computing contract are usually adopted in your jurisdiction, including cloud provider supply chains (if applicable)?

Usually, the supplier's standard cloud computing contract is applied. Given the bargaining power of the customer, the cloud computing contract may, in rare cases, be based on the customer's standard template, in particular, when the supplier is a local cloud provider. Notwithstanding the above, for certain areas of the cloud computing contract, the suppliers, including international cloud providers, have become more recipient towards implementing customer requirements in the contract. This relates in particular to regulatory requirements, such as requirements deriving from privacy legislation and regulations, requirements on public sector entities and financial regulations.

Typical terms for governing law

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering governing law, jurisdiction, enforceability and cross-border issues, and dispute resolution?

As cloud computing contracts are often drafted on the basis of the supplier's standard cloud computing contract, governing law will, in many cases, be the law that applies where the supplier's business is based, such as the laws of Ireland or the US. However, you may also find contracts that are governed by Swedish law, in particular from local Swedish cloud suppliers, but also larger international enterprises that have opened up local Swedish entities.

For data privacy, Swedish law will typically apply, in particular since this is a regulatory requirement from the Swedish DPA or at least that was the case prior to the GDPR. As to jurisdiction, principles corresponding with those above would normally apply. In most Swedish B2B contracts, arbitration is used as a method of dispute resolution and this would typically also apply to cloud computing contracts. Ultimately, the choice of rules for dispute resolution as well as governing law and jurisdiction would be the result of the parties' negotiations. Many of the larger cloud service providers will not accept that the agreement will be governed by Swedish law. The enforceability of a cloud service contract is, however, uncertain as there is very limited case law regarding this matter.

Cross-border issues are mostly discussed in respect of data privacy and secrecy. Data privacy cross-border issues are usually regulated through the use of the standard contractual clauses decided by the EU Commission on 5 February 2010 (2010/87/EU) that supplement the cloud computing contract to allow transfer of personal data outside the EEA. Many cloud service providers are reluctant to provide a guarantee that data will not be processed outside the EU and EEA even if they may commit to mainly use data centres within the EEA as their main facilities for the services. The newly adopted US Cloud Act, giving US authorities a right of access to data that is stored by US cloud service providers worldwide, is likely to add to the complex landscape.

Typical terms of service

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering material terms, such as commercial terms of service and acceptable use, and variation?

Commercial terms of service and acceptable use are commonly agreed on the basis of the supplier's standard cloud computing contract. Price model and payment terms vary depending on the services offered, however, services are commonly purchased as subscriptions and invoiced in advance. Provided that payment is overdue, the supplier may reserve the right to suspend the services immediately, however, sometimes excluding cases where payment is withheld in good faith. Principles for acceptable use commonly include customary restrictions, such as prohibition against redistribution of the services, use of the services for provision of outsourcing services and transmission of infringing material or malicious code.

As to variation, the supplier's standard cloud computing contract will, in many cases, include the unilateral right for the supplier to change the services, including the functionality and security. Such provisions may often be the subject of negotiations between the parties, for example, when the customer is a regulated entity and the provisions are in violation of the regulatory requirements applicable to the customer.

Typical terms covering data protection

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering data and confidentiality considerations?

In terms of data, cloud computing contracts have in recent years been greatly influenced by the statements and decisions of the Swedish DPA regarding the processing of personal data by cloud computing suppliers. These statements and decisions prescribe, among other things, that the customer must ensure that:

- a sufficient data processor agreement is entered into with the supplier;
- the supplier is not allowed to independently process personal data but only in accordance with the customer's instructions;
- the contract stipulates that Swedish law applies as regards the processing of personal data; and
- the customer is informed of all sub-processors involved in the processing of personal data type of services and the location of such sub-processors.

In addition, the customer should ensure that it is entitled to perform audits for the purpose of ascertaining the supplier's compliance with the customer's requirements on the processing and that a process for exit of the agreement is established, which safeguards that the supplier will not process the personal data post termination of the contract.

Moreover, the customer is, as a general rule, obligated to perform a legality assessment and risk and vulnerability analysis prior to entering into the cloud computing contract. The purpose of the legality assessment is to determine whether the supplier's processing of personal data under the cloud computing contract will be allowed under the data protection legislation. This includes measures such as ensuring that a data processor agreement is

entered into, an assessment regarding cross-border transfers and any security measures necessary. The purpose of the risk and vulnerability analysis is to assess whether it is possible to assign the processing of personal data to the supplier and determine appropriate security levels and necessary measures that need to be taken in the light of the integrity risks involved.

Following the entering into force of the GDPR, it is currently not clear whether the above principles will be upheld by the Swedish DPA.

Confidentiality provisions are commonly mutual.

Typical terms covering liability

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering liability, warranties and provision of service?

Since the cloud computing contract in many cases is based on the supplier's standard contract, the supplier's warranties are normally limited. A typical warranty would imply that the services are materially consistent with the documentation, and that the supplier will not materially change the functionality of the services or the security of the services. Ultimately, the warranties may be subject to negotiation between the parties.

Limitation of liability is often mutual with a cap and excluding indirect and consequential damages. There is normally a carve-out for liability for death and personal injury and damages caused by intent or gross negligence. In some agreements, liability for breach of confidentiality is uncapped but with a carve-out for loss of customer data entered into the cloud services, which instead falls under the general liability in the agreement.

The supplier would normally provide indemnities for intellectual property rights (IPR) infringements caused by the proper use of the services and, correspondingly, the customer would provide for the IPR infringements caused by the proper use of customer data. You may also find other types of indemnities (eg, in case of violation of applicable law or customers' misuse of the services).

Service levels is a typical area where the cloud computing contracts are less flexible and the customer will in many cases have to accept the supplier's standard SLAs. Penalties and similar possible remedies in the event of non-fulfilment of the SLAs are often limited to fairly low amounts and are sometimes a customer's sole remedy for such non-fulfilment.

Business continuity and disaster recovery plans could be necessary to implement as a result of the risk and vulnerability analysis performed by the customer prior to entering into the cloud computing contract and this would also normally be required by customers that are regulated entities.

Typical terms covering IP rights

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering intellectual property rights (IPR) ownership in content and the consequences of infringement of third-party rights?

The supplier generally reserves the IPR to the services and non-customer-specific content, whereas the customer reserves the IPR to customer data. Customary consequences of infringement of IPR normally apply (ie, modification of the services so that they are no longer infringing, obtaining a licence for the customer's continued use of the services or, ultimately, termination of subscription and refund of licence costs). The customer is often undertaking to indemnify the supplier for any claims made towards the supplier due to the content of the customer data entered into the services.

Typical terms covering termination

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering termination?

Either party will typically have the right to terminate the cloud computing contract in case of material breach of the contract by the other party. Additionally, the customer often has the right to terminate the contract in cases where the supplier appoints a sub-processor that the customer on objective grounds refuses to accept. Following termination of the contract, the supplier will no longer have a right to process personal data for which the customer is the controller; however, the supplier is usually allowed a certain period of time to remove such data (up to 180 days are often seen, but it remains to be seen whether this period will change given the GDPR).

The supplier may offer migration services on a time and material basis.

Employment law considerations

Identify any labour and employment law considerations that apply specifically to cloud computing in your jurisdiction.

The Acquired Rights Directive 2001/23/EC would (at least in principle) apply to a business customer entering into a cloud computing contract, provided that the cloud computing services are deemed to be outsourcing.

Taxation

Applicable tax rules

Outline the taxation rules that apply to the establishment and operation of cloud computing companies in your jurisdiction.

Cloud computing companies are subject to the taxation rules generally applicable to companies in Sweden. An international cloud computing company providing services to Swedish customers may be subject to Swedish taxation, provided it can be held to have a permanent establishment in Sweden. Subject to the nature of the payment under the cloud computing agreement, withholding tax issues may arise that need to be addressed in the cloud computing agreement.

Indirect taxes

Outline the indirect taxes imposed in your jurisdiction that apply to the provision from within, or importing of cloud computing services from outside, your jurisdiction.

VAT (25 per cent) will be imposed on provision of cloud computing services from within Sweden. In respect of cloud computing services provided within the EU, a reverse charge will, as a general rule, apply. Specific rules apply for cloud computing services provided from outside the EU.

Recent cases

Notable cases

Identify and give details of any notable cases, or commercial, private, administrative or regulatory determinations within the past three years in your jurisdiction that have directly involved cloud computing as a business model.

There is limited case law in Sweden regarding the use of cloud computing. Most case law is based on disputes regarding public procurements. In one notable case from the Administrative Court in 2014, the Court found that there had been shortcomings in a Swedish municipality's agreement with Google regarding the use of cloud services by a public school.

Update and trends

Update and trends

What are the main challenges facing cloud computing within, from or to your jurisdiction? Are there any draft laws or legislative initiatives specific to cloud computing that are being developed or are contemplated?

The main challenge in the next few years, in respect of cloud computing services, is to ensure compliance under the GDPR while using and providing cloud computing services. Notably, many cloud suppliers have been swift to ensure that their contracts comply with the requirements under the GDPR for data-processing agreements.

The new US Cloud Act conflicts with the GDPR and is likely to have an impact on organisations' choice of cloud suppliers going forward. As of August 2018, the Swedish DPA has not yet taken a stance in respect of the Cloud Act and the uncertainty as to its implications is used as a sales argument by many local Swedish cloud suppliers.

Another challenge is that many cloud suppliers are - sometimes due to their position in the market, strict (US) corporate policies or because the Swedish market is fairly limited in size - very restrictive with accepting any amendments to their contractual documents at all. If the supplier is not willing to discuss or make any additions or amendments to its terms, this could very well spell the end of and organisation's relationship with a particular cloud service, since many of the terms and conditions offered by cloud suppliers may not fulfil all the legal requirements required for the entity to be able to use the services. This is a particular challenge for entities governed by sector-specific rules, such as financial institutions, entities within the health sector and public entities.

The challenge for banks and other financial institutions, is that the Swedish regulatory authority, the Financial Supervisory Authority, considers cloud services to be a form of outsourcing and, as a result, specific regulatory requirements for outsourcing must be met in order to be able to use these services. Owing to the nature of cloud services and the content and form of the cloud suppliers' standard terms and conditions, fulfilling these requirements may be difficult. As mentioned above, entities within the public sector are also struggling with whether their use of cloud services are compatible with undertakings regarding statutory secrecy under the Secrecy Act (SFS 2009:400).

Another challenge is that cloud service providers in general are reluctant to provide more detailed information regarding the security of the services. Information of third-party reports, its business continuity and disaster recovery plans are crucial to assess the risks and to determine the possibility of using the services.

The rules in the GDPR will likely have a great effect on the use of cloud services. The Financial Supervisory Authority is regularly providing financial institutions with guidance on how the adaptations of the requirements on outsourcing are to be applied in a cloud environment. In addition, there are ongoing discussions on public entities' use of cloud services in light of their obligations under the Secrecy Act (SFS 2009:400). It is hoped more clarification on the government's position regarding these matters can be expected in the near future.

It should also be mentioned that the National Government Service Centre, under the authority of the Swedish government, issued a report in February 2017 with a proposal to implement a governmental cloud service. The purpose of such cloud service, according to the report, is to set up secure national cloud services that all government entities (more or less) will be obliged to use for hosting services and similar cloud-related services. No formal decision on the proposal in the report has been made but, in August 2017, the Swedish government assigned the Swedish Social Insurance Agency to set up and offer centralised national hosting services for use by Swedish government agencies. Pursuant to the decision, the use of such services will be optional and the assignment runs until 2020.

Advokatfirman Delphi - Dahae Roland and Peter Nordbeck