Norwegian Ministry
of Local Government
and Modernisation

Strategy

Cloud Computing Strategy for Norway

Foreword

Norwegian public and private enterprises outsourced services for many years. This allows them to focus on their core activities and leave for example IT services to an external party. In recent years cloud computing has become an important outsourcing alternative. We see that a growing number of both infrastructure and software services are being supplied in the cloud. This also applies to services aimed at the public sector.

One could ask whether we need a separate strategy for cloud services; after all, we have been outsourcing services for many years now. However, cloud services differ from traditional outsourcing models in important areas which create challenges for enterprises considering using such services and, in particular, for public sector enterprises: it is not always possible to know exactly where or when data is stored or processed, and the agreements regulating these services are often standard contracts issued by the service providers. Many enterprises have concerns about the security of cloud services and whether current regulations permit their use.

The public sector must become more cost-effective in the coming years, and the use of ICT and the digitisation of services constitute a vital element in this process. But the operation of digital services and public ICT systems must also be cost-effective. In the *Circular on digitisation* for 2016, which applies to all public sector enterprises, we therefore require that they consider cloud services as an alternative when procuring ICT. In this strategy we propose measures to make it easier for both public and private enterprises to conduct this type of assessment.

It is also important that public sector enterprises operate their ICT systems reliably and securely. A key element of the development of this strategy has been to assess existing legislation to ensure that it makes clear what is permissible and what is not. In following up this strategy, we will establish resources that can provide guidelines for procurement of cloud computing on topics such as: information value assessment, information security, risk assessment and contract management for the public sector. Such resources will also have transfer value for business and industry.

During the development of this strategy the Ministry of Local Government and Modernisation has held workshops with public sector enterprises, municipalities and the ICT industry, as well as regular meetings with an advisory group with representatives from central government, local government and key stakeholders in data protection and security. During the same period, the Norwegian Association of Local and Regional Authorities has conducted a feasibility study of the use of cloud computing in the municipalities. The two projects have cooperated closely. I would like to thank everyone involved for providing important input.

Jan Tore Sanner
Minister of Local Government and Modernisation

Contents

1 Introduction and summary

Future growth and welfare in Norway is contingent on continued increase in productivity.[1] Two key factors for growth are innovation and new business development. In order to meet future requirements for public services, we need to make better use of technology. The private sector, particularly service industries, needs to improve at adopting new technology to ensure continued increase in productivity.

Public sector enterprises vary widely in terms of needs, risk profiles, financing and available expertise. One thing they have in common is a responsibility to choose the most appropriate and cost-effective ICT solutions that meet their needs. It goes without saying that the same applies to business and industry.

The public sector has a duty to operate as cost-effectively as possible, but it also has a responsibility to properly safeguard citizens' personal data and to protect their interests. It is therefore important that all available solutions be assessed – including cloud computing – when deciding which ICT solutions to procure. Services from the public cloud will suit some enterprises, but not all. The best solution is often a combination of delivery models.

When enterprises are asked about their motivation for considering cloud computing, the usual answers are reduced costs and increased flexibility, but a third answer we are hearing more often is: "This is how solutions are being supplied now. If we are to have the latest version of the systems we want to use, then we have to choose cloud services." Cloud computing can reduce the need for investment and thus reduce the risks associated with establishing a new business or developing new services.

However, many enterprises – both public and private – find it difficult to know whether cloud computing is legally permitted and sufficiently secure. And is it really acceptable to store personal data abroad? The Government's aim for this strategy is to clarify questions like these.

Strategy objectives

The main objective of the *Cloud Computing Strategy for Norway* is to provide public and private enterprises with more room for manoeuvre when deciding which ICT solutions to use. Provided that other important considerations are not compromised, enterprises should be able to use cloud services wherever they promise the best result and the most cost-effective solution.

The strategy should facilitate:

- more cost-effective ICT solutions
- increased focus on core activities
- greater flexibility
- greater security through more professional and standardised ICT
- lower threshold for innovation and startups
- reduced carbon footprint from ICT operations

[1] NOU 2015:1 *Produktivitet – grunnlag for vekst og velferd* [Productivity – Underpinning Growth and Welfare]. First report of the Productivity Commission.

Target group for the strategy

This strategy is aimed at all enterprises, both public and private. Much of the strategy is directly aimed at the public sector, but these parts will also have transfer value for business and industry. Not least, it will be important for those segments of the private sector delivering ICT solutions to the public sector to know what principles public sector enterprises must follow when procuring new ICT services.

The strategy is not aimed particularly at consumers. While there are several interesting issues related to cloud services for consumers, they are not within the scope of this strategy. Such issues fall under the mandate of the Ministry of Children and Equality and the Norwegian Consumer Council.

Summary

The strategy is structured in such a way that the general sections – those addressing both the public and the private sectors – are presented first.

Chapter 2 discusses important features, benefits and challenges of cloud computing. This chapter also discusses some important general considerations that must be taken into account when procuring cloud services.

One important part of the work done on this strategy has been to review Norwegian legislation to identify any obstacles to the use of cloud services, and to assess whether something should be done about them. It is also important to look at areas where legislation is complicated or vague and assess whether laws and regulations relating to cloud computing can be clarified.

The legal review has resulted in some important measures:

- Revision of the Regulations pursuant to the Public Archives Act and, where appropriate, sections of the Public Archives Act to better adapt archiving regulations to digitisation. One point to be considered is the need for amendments to allow public bodies to use cloud services with servers located outside Norway for archiving purposes.
- Assessment of the possibilities for expanding the number of countries where book-keeping data can be stored legally. Important measures in this area are already under way in the European Union (EU), and Norway will monitor developments closely.
- Efforts to harmonise supervisory practices as far as possible, so that enterprises do not encounter conflicting requirements issued by different supervisory authorities.
- Input to the EU's work on establishing common criteria (standards, certification schemes, etc.) for cloud services.

The legal challenges are discussed in more detail in chapter three.

The Government has already implemented one key measure addressing cloud services. The *Circular on digitisation* for 2016, which was issued to all public agencies, included the principle for using cloud computing:

- *Cloud computing shall be assessed on the same basis as other solutions when considering major changes or reorganisation of ICT systems or operations:*
  - *when procuring new systems or performing major upgrades*
  - *when undertaking extensive replacements of hardware*

  - *when existing operating agreements expire*
- *When they offer the most appropriate and cost-effective solution and when no particular obstacles stand in the way of using them, cloud services should be chosen.*
- *The chosen solution must satisfy the agency's requirements for information security. This means that enterprises must know the value of its own systems and data, and perform a risk assessment of the chosen solution.*

The principle for using cloud computing is discussed in more detail in chapter 4 Conditions for using cloud computing in the public sector.

Chapter 4 also discusses control issues relevant to the public sector, as well as what control mechanisms exist for cloud computing. We also present measures that will make it easier for public sector enterprises to assess cloud services:

- Resources to support enterprises in assessing and procuring cloud services.
- A project to identify and evaluate different models for a potential marketplace and/or procurement framework for cloud computing services aimed at the public sector.
- The Government also wants to facilitate better utilisation of existing public data centre resources, in particular for agencies with such security requirements that they are considering buying high-security data centre services or establishing their own data centres in Norway. In such cases, agencies must assess the possibility of utilising free capacity from – or cooperating with – other agencies with similar needs.

2 What is cloud computing?

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The buying of services from external providers is not something new. The risk involved in using cloud services is essentially the same as that for traditional outsourcing of ICT operating services, where risk and vulnerability are associated with the choice of provider, location, communication channels and architecture.[2]

The Government has chosen to use the NIST (National Institute of Standards and Technology) definition of cloud computing.[3]

NIST defines the following characteristics of cloud computing:

- *On demand self-service*
  A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- *Broad network access*
  Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling*
  The provider's computing resources are pooled to serve multiple consumers, dynamically assigning physical and virtual resources according to consumer demand.
- *Rapid elasticity*
  Capabilities can be elastically provisioned and released according to demand. They appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service*
  Resource usage is monitored, controlled and reported, providing transparency for both the customer and the service provider.

Five characteristics	Three service models	Four deployment models
On-demand self-service Broad network access Resource pooling Rapid elasticity Measured service	Software as a Service (SaaS) *Desktop applications, CRM, accounting* Platform as a Service (PaaS) *Databases, development platforms, operating systems* Infrastructure as a Service (IaaS) *Storage, processing, virtualisation*	Public cloud Community cloud *Similar enterprises share a cloud* Private cloud Hybrid cloud *Public cloud combined with private cloud/community cloud*

[2] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* [Digital Vulnerability and a Secure Society].

[3] Mell, Peter and Grance, Timothy (2011): *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce, NIST Special Publication 800-145.

Example: UNINETT – a cloud broker for the higher education sector

UNINETT is owned by the Norwegian Ministry of Education and Research, and provides internet access and online services to the higher education sector in Norway. In 2016 the ministry has commissioned UNINETT to establish a community cloud for Norwegian universities and university colleges. UNINETT will therefore serve as a cloud service broker for the entire higher education sector and provide secure cloud services, including adapted commercial cloud services.

UNINETT has already established a community cloud (UH-sky) in collaboration with the Universities of Trondheim, Oslo, Bergen and Tromsø. The work on developing the cloud brokerage service will continue this collaboration.

UNINETT is also working on cloud-based infrastructure platforms to make typical data-centre services accessible from the cloud. Moreover, some universities are cooperating on establishing a common infrastructure platform in their data centres so that they can provide infrastructure services to other actors within the sector in the future.

Source: UNINETT

Service models

Different service models are available in the cloud, depending on enterprise needs. Software or applications that are running on the provider's cloud infrastructure are known as *Software as a Service* (SaaS). Using software hosted in the cloud means that customers are spared having to buy, install, update and maintain software locally. Instead, users can run applications through their web browser or another thin client. Examples of SaaS are desktop applications such as word processing and spreadsheets, accounting and CRM systems.

Platform as a Service (PaaS) offers everything needed to support creating and deploying digital services, such as programming languages, libraries and tools supported by the provider. A platform can be a database or an entire development or test environment.

Infrastructure as a Service (IaaS) provides all the data resources customers normally need in their own data centre or server room: storage, networks and other fundamental computing resources. Although buying SaaS and PaaS is gradually becoming widespread, buying storage and processing capacity is still more commonplace.

Deployment models

Cloud services can be provided through different deployment models:

Public cloud infrastructure provisioned for open use by the general public. The public cloud provides standard solutions that are largely the same for all customers. The biggest and best-known providers are Google, Amazon and Microsoft.

Public cloud can also be integrated with the architecture of software service providers – including Norwegian providers – who provide software as a service. An enterprise can therefore end up using services from the public cloud even if this was not explicitly a part of the service purchased.

A *private cloud* is provisioned for exclusive use by a single organisation or group of enterprises (often referred to as a *community cloud*). The environment from which the cloud service is

provided is dedicated to a specific customer or customer group. An organisation can also operate its own cloud, but unless it is sufficiently large, it will not achieve the same economies of scale as with a public cloud. On the other hand, it will not be exposed to the same risks.

If an enterprise uses a combination of public cloud and locally operated ICT systems, a private cloud or a community cloud, this is known as a *hybrid cloud*.

Most enterprises have information which, for various reasons, they are reluctant to store in a public cloud. This may be business-critical information or information that cannot be stored abroad under current regulations, or data that would take too long to process elsewhere. At the same time, the public cloud can be a good alternative when the need arises for extra capacity or storing back-ups, or for hosting systems that are non-business-critical or that contain information that must be stored locally. An architecture with a hybrid cloud enables enterprises to take advantage of the benefits of a public cloud while at the same time retaining control over business-critical components. Hybrid cloud is the deployment model currently experiencing the fastest growth.[4]

This strategy focuses mostly on discussing the issues associated with using *public cloud*. Clarifying what is legally permitted and recommended when it comes to the public cloud is transferable to other models, such as community cloud or hybrid cloud where public cloud is an integral part of the architecture.

Benefits and challenges of cloud computing

Cost savings is one of the most common benefits associated with cloud computing. It has also been the motivation in many countries where governments have already established an ICT strategy in which cloud computing play a key role. For example, the UK has implemented a cloud-first policy,[5] and expects the transition to affordable, standardised ICT solutions to reduce ICT costs in the public sector.

In a study commissioned by the Norwegian Association of Local and Regional Authorities,[6] the responding municipalities considered the main drivers for adopting cloud computing to be: financial, a wish to focus on service development, scalability and flexibility, and more accessible to municipal services for citizens.

Cost-effectiveness

Many automatically think of reduced costs when cloud computing is mentioned. There are several reasons for this: the fact that a cloud service requires no local infrastructure affects the cost of investing in and operating ICT. Cloud computing can also lead to reduced costs for updates, administration of software licences, etc.

The pricing model for cloud services, which entails measuring and paying for use, also makes the costs for each service transparent. Customers avoid having to pay for more computing power, more storage space or more programme licences than needed at any given time. Such

[4] Rightscale (2016): *State of the Cloud Report.*

[5] HM Government (2011): *Government Cloud Strategy. A sub strategy of the Government ICT Strategy.*

[6] Advokatfirmaet Føyen Torkildsen AS (2015): *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie* [Report on the legal aspects of cloud computing in the municipal sector: A feasibility study]. Norwegian Association of Local and Regional Authorities R&D project no. 144008.

Example: Moss Municipality

Moss Municipality has a population of 32,000 and 2,500 employees. It administrates around 100 IT systems and uses 8.2 full-time equivalents on ICT.

The municipality had to acquire several additional e-mail licences to provide all its employees with e-mail accounts. It discovered that using Office 365 in the cloud cost far less than using equivalent software installed locally. The municipality has opted for a hybrid solution whereby parts of the system portfolio (including archives) are operated locally while, for example, desktop applications are operated in a public cloud service (Microsoft Azure). Although it also considered traditional outsourcing, the municipality concluded that this would prove far more expensive than a cloud solution and more expensive than continuing to operate IT locally.

Source: Moss Municipality

a pricing model is particularly favourable for enterprises that have processes requiring large capacity but only for short periods of time; for example, monthly or annual tasks such as issuing invoices or performing payroll runs.

Not all enterprises that adapt cloud services find them cheaper than other alternatives. This particularly applies for enterprises with special requirements that cannot be provided as a standard solution or where a cloud service will be part of a complex architecture with extensive integration with existing systems.

Scalability

Cloud services offer practically unlimited capacity for data processing and storage. The resources in the cloud are allocated to the customer organisations only when needed. This means that enterprises need not worry about running out of capacity if, for example, a public service it provides is used more than anticipated. This is also an advantage for enterprises with services that are vulnerable to overload during peak periods, often without being able to foresee their occurrence.

The elements that make cloud services cost-effective and scalable can also create challenges for enterprises administrating personal data, confidential information or information in areas where regulatory restrictions apply as to which countries data can be transferred. In order to offer affordable services, providers make use of any free capacity they have in their systems. Consequently, enterprises can never know which data centres – or countries – their information is stored in at any given time. It may also be the case that a cloud software service provider uses multiple subcontractors without this being clearly stated in the service specification.

Security

Cloud computing can enhance technical ICT security when the service provider has better expertise and resources than the customer.[7] This applies not least to the physical security of premises where hardware is located. Large data centres generally have comprehensive security measures in place, and heavy restrictions on who may enter the premises. Service

[7] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* [Digital Vulnerability and a Secure Society].

Example: Banedanmark

In December 2010 Banedanmark (the Danish rail network provider) migrated its website to a cloud service (Microsoft Azure). That winter, Denmark's transport services experienced major problems. While other transport companies found that their information services failed due to the dramatic increase in enquiries from the public, this did not happen to Banedanmark. At most, it had 5.5 million users in one day compared with the normal 50,000. The company paid DKK 179 for the increased capacity it needed during this period.

Source: Centre for Digital Administration (2013): *Public sector use of cloud based solutions – the Danish experience*. Survey commissioned by Microsoft.

providers replace hardware and upgrade software regularly. There are certification schemes for data centres indicating which security level a data centre meets.

When software is provided in the form of a cloud service, this often means that the customer is provided with a standard solution. It also means that all customers receive security updates and other software updates simultaneously. For many customers this can enhance security because they previously lacked sound procedures for such updating.

Back-ups are normally part of a service portfolio when buying cloud services. Redundancy and automatic transfer to a new location should something go wrong in the primary location are other services often offered as standard.

A type of service that is growing in popularity is *Security as a Service* (SECaaS). Through SECaaS enterprises can subscribe to various types of security services such as anti-virus programmes and continual anti-virus updates, authentication, malware detection, and administration of security events.

Although cloud computing can in many cases enhance security, it is important that enterprises assess whether some of their information needs extra security measures for financial, competitive or other reasons. Many enterprises may also find it relevant to assess the security policy consequences of using cloud services based outside the European Economic Area (EEA). Some national authorities allow greater access to foreign data than to data pertaining to their own citizens and enterprises. Even enterprises that are not subject to the Security Act may find it relevant to consider such matters.

It is worth mentioning that information which is not deemed sensitive in itself may be deemed sensitive if stored in a common data centre or a cloud service where information belonging to other societal functions is also stored. The potential harm through loss of the collective information could have ramifications for national security. This can make risk assessments more complicated, since an enterprise risks having to assess not only its own data but also the consequence of storing too much public information in the same location.

Many enterprises feel safer having their own servers and data close to home, and fear losing control if their data is stored and processed in a distant – and perhaps unknown – location. This issue can be addressed through various control mechanisms, as discussed in detail in chapter four.

Energy efficiency

Providers of services in the public cloud can allocate their hardware resources to a large number of customers. This makes for more efficient energy consumption than if all the customers had their own data centres with their own hardware, cooling systems, etc.

The current trend is for providers of cloud and data centre services to consolidate their data centres into large and increasingly energy-efficient entities. These data centres are often located in areas with stable access to cheap energy.

Flexibility

In many cases, cloud computing makes it easier to enable services (such as a municipality's case processing system) to be used from different locations and from different client types (PC, tablet, mobile phone).

Both public and private enterprises are increasingly allowing their employees to use their own PCs, tablets, etc. This policy is often referred to as *Bring Your Own Device* or *BYOD*. BYOD poses new challenges in terms of security and availability. Cloud services can make it more convenient for users to store their work on their enterprise's storage area in the cloud instead of locally on their personal equipment, outside the control of the enterprise. Most enterprises have employees who already use unauthorised consumer cloud services in order to give them flexibility in their working day. This poses a risk to the enterprises, not least because end-user licence agreements in the consumer market often give service providers wide authority for what they may do with their customers' data.

As enterprises gradually buy more services in the cloud, this will affect the need for local expertise. This may lead to reduced expertise in some areas because employees no longer work in those areas on a daily basis. On the other hand, it could spare key personnel from having to perform routine tasks and allow enterprises to devote more energy internally to strategic planning and service development.

Innovation

Cloud services can reduce the scope of investments needed to start up new enterprises. Because no major investments are needed in hardware and infrastructure or software licences, there will be less need for startup capital.

This is particularly relevant when starting up an enterprise providing services to customers over the internet: it can be difficult to estimate how many customers will come and how fast. Nonetheless, not having sufficient capacity to provide a service can be risky if the service quickly proves to be a success. A cloud-based infrastructure that can be scaled up or down according to the expected number of customers and that is based on a pay-as-you-go model will reduce the risk of loss on infrastructure investments. Such a model also allows enterprises to take the time to adapt and further develop a service if it fails to prove successful immediately.

For the same reason, cloud services can make it easier for existing enterprises to set up platforms for development and innovation, such as test environments or pilot projects. This can lower the threshold for testing new solutions, both internally and for customers.

Example: Comoyo

Comoyo was Telenor's venture into streaming services. The service was established as early as 2011.

As recently as in May 2013 Telenor announced: "With the newly established Comoyo, Telenor will capture 130 million consumers in all channels and on all platforms." Telenor closed down Comoyo in November 2013 after major international players like Netflix and HBO established themselves with streaming services in the Nordic countries and captured most of the market.

Telenor used Amazon's infrastructure to provide the service, which meant that it only paid for the capacity it needed to serve the customers it had at any given time. Consequently, when the service was discontinued, Telenor was not left with large investments in infrastructure the company no longer needed.

Sources: Teknisk Ukeblad/Comoyo/Telenor

For the public sector, such platforms can make it easier to test and adopt new public services. This is particularly important for the municipalities, as they often have few resources to allocate to tasks like these. In this way cloud computing can contribute both to rationalisation and service development in the public sector.

Important considerations before procuring cloud services

The Government wants to make it easier for public and private enterprises to consider cloud computing as an alternative when procuring new ICT systems. A key premise for doing this is clarifying the regulations, as discussed in chapter 3. However, other factors not directly related to regulatory matters must also be taken into account when considering cloud computing.

Sourcing

The strategic decisions an enterprise makes regarding which services to buy from external providers and which services to manage itself for strategic reasons constitute the enterprise's *sourcing strategy.*

Such strategies involve not only ICT; an enterprise may also decide to outsource functions such as finance and accounting, logistics, or other tasks the enterprises does not regard as core activities. This is often referred to as *outsourcing.* One reason for outsourcing services might be to achieve economies of scale, making it more cost-effective for the enterprise than having to produce the services itself.

Procurement of cloud services is a form of sourcing, as is an enterprise's decision to produce or operate its ICT solutions internally. Whichever sourcing strategy an enterprise chooses, an analysis is needed to decide whether the chosen solution meets current requirements for the type of information the system will process and whether the risk associated with the chosen strategy is acceptable. Assessing risk or making sure a data processing agreement is signed are not tasks that are specific to procuring cloud services; they need to be done regardless of the chosen strategy.

Architecture

The Agency for Public Management and eGovernment (Difi) has defined a set of principles[8] to serve as common guidelines for all use of ICT in the public sector. Public agencies are required to follow the principles, whereas the municipal sector is recommended to do likewise.

Although an agency might not find cloud services that currently meet requirements for the system it wants to develop or buy, by following Difi's architectural principles it can make sure that it does not preclude cloud computing as its chosen platform later on.

The key principles for ensuring that a chosen strategy does not preclude the use of cloud computing are:

- *Interoperability*: Involves using technical standards that facilitate well-defined interfaces, transmission protocols and formats.
- *Flexibility:* ICT solutions shall be designed in such a way that they do not pose barriers against changes in business processes, content, organisation, ownership or infrastructure.
- *Scalability:* ICT solutions must be scalable to accommodate changes in use. Changes can be related to, for example, the number of users, volume, response times, etc. It must be possible to scale the solution up or down after it is put into operation.

The other principles – such as security and service orientation – are of course as important and relevant for any ICT project for which cloud computing is being considered as for other types of projects.

If an enterprise is to develop new, local systems, it is important to choose an architecture that can benefit from the typical advantages of cloud computing and that is suitable for migrating to the cloud if desired at a later date.

Information security

The security assessments that must be made when considering cloud computing are not that different from those that need to be made when outsourcing to an external service provider. In practice this means that the enterprise must carefully consider the formal guarantees the service provider gives, such as where data will be stored or processed.

The risk associated with using cloud services will vary according to where sensitive data is to be stored or processed and how the chosen cloud service provider has implemented its cloud services. To what extent the provider should be assessed will depend on the value of the information involved and how serious the consequences might be if something went wrong.

Information security has to do with how to maintain the confidentiality, integrity and availability of information.[9]

Integrity is the assurance that data is comprehensive, accurate and valid. Integrity also assures that no unauthorised changes are made to the data.

Confidentiality is assurance that information is not disclosed to unauthorised parties and that only authorised persons – that is, people with the right to – gain access to it.

---

[8] Agency for Public Management and eGovernment (2102): *Overordnede IT-arkitekturprinsipper for offentlig sektor* [Overarching IT architectural principles for the public sector] Version 2.1, 17 September 2012.

[9] Norwegian Ministry of Government Administration, Reform and Church Affairs (2013): *Cyber Security Strategy for Norway*

Availability is assurance that a service meets specific requirements for stability so that the information is available when needed.

Previously, security concerns were mainly associated with confidentiality, the main concern being that unauthorised persons could, for example, gain access to business secrets or sensitive information on individuals. We now see that concerns about integrity are increasing. Unauthorised modification of data can occur as the result of either technical factors or malicious attacks. If an enterprise does not trust the integrity of its system, there may be serious consequences if the information is used for making important decisions or if, for example, the information is stored in a system that is critical for the enterprise or its customers.

As society becomes increasingly dependent on having access to ICT and networks in order to function, availability will also become increasingly important when considering information security issues. If a key service is not available over time, this can have serious consequences for an enterprise. Many enterprises have critical systems that do not tolerate any downtime whatsoever.

Moreover, the commission appointed to assess digital vulnerabilities in society (see text box) raised a fourth security objective: *traceability.*[10] Traceability has to do with finding out what happened in retrospect; for example, by using change logs or other event logs.

Public enterprises must – and private enterprises should – perform risk and vulnerability analyses when planning major changes such as new digital services, reorganising system operation, changing service provider, etc. This requirement applies to all enterprises that process personal data. The enterprise must assess what consequences different events may have for its users, for the enterprise itself, and for the sector as a whole. The enterprise must then assess the likelihood of these events occurring. The risk level is determined by a combined assessment of the consequences of the events and the likelihood of them actually occurring.

Similarly, each enterprise must assess what the consequences would be if a security breach occurred along the three information security dimensions – availability, confidentiality and integrity: What will happen if a system or service is unavailable for a given time period? What are the possible consequences if an unauthorised party gains access to the information? What are the possible consequences if unauthorised parties manage to modify the information so that it can no longer be trusted? What is the likelihood of the individual consequences occurring? Which consequence constitutes the greatest risk? What requirements should be set to an internal or external provider for managing such risk?

The purpose of a risk analysis is to help an enterprise that is considering cloud computing to make an informed assessment of whether the risk level associated with using cloud services is acceptable. Such assessments must also be performed for other forms of sourcing where an enterprise must hand over control of its data to an external partner.

[10] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* [Digital Vulnerability and a Secure Society].

Commission on Digital Vulnerability

In June 2014 the Government appointed a commission to examine digital vulnerabilities in society (Lysne Commission). The commission presented its report to the Norwegian Minster of Justice and Public Security on 30 November 2015.

Some of the issues relating to cloud computing discussed in the report are:

- Large, established cloud computing providers can often offer better security than what many small organisations can manage themselves. This will of course depend on the provider. The user is responsible for assessing whether the information it intends to store in the cloud is vulnerable if transferred outside Norwegian jurisdiction, and must weigh the consequences and risk against the benefits.
- The government authorities must not make it difficult to adopt practical and cost-effective technology as long as there are solutions that are sufficiently secure. It is important that Norwegian legislation not impede increased competitiveness.
- Section 9 of the Public Archives Act, which states that archives may not be transferred out of the country, was introduced over 20 years ago, and therefore does not take into account modern-day technology developments and needs.

Commission recommendations

Information can be divided into three categories:

1. Information that should only be stored in Norway
2. Information that can be stored abroad but that can be returned to Norway if necessary, subject to specific conditions
3. Information that can be stored abroad without being subject to specific conditions

Category 1: Information that should only be stored inside Norwegian territory and jurisdiction applies particularly to classified information. The commission concludes that each sector must assess which information falls under the respective categories. The commission also emphasizes that the sectors will in many cases find it difficult to coordinate with each other, so there is a need for standards and guidance across the sectors.

The commission highlighted the need to harmonise supervisory practices across the sectors. This work should include taking a closer look at the use of third-party audits.

Source: NOU 2015: 13 *Digital sårbarhet – sikkert samfunn* [Digital Vulnerability and a Secure Society].

Data protection

It is important to check that the data processing agreement used meets the requirements stipulated in the Personal Data Act. Once the new General Data Protection Regulation (see chapter 3) enters into force, making the same regulations applicable to all processing of personal data on citizens in the EU/EEA, service providers will likely issue more standardised agreements.

Note that it is *always* the enterprise itself (the data controller) that is ultimately responsible for ensuring that information be properly processed. This responsibility is not transferred to the provider, even when all agreements are signed. Under the new General Data Protection

Regulation the provider (data processor) also has a responsibility, but that does not replace the responsibility of the data controller.

The Norwegian Data Protection Authority has prepared a checklist with issues enterprises must consider before they begin using cloud services for processing personal data.[11] The checklist is based on legislation and best practice.

- The enterprise must perform thorough risk assessments, including risk and vulnerability analyses.
- The enterprise must enter into a satisfactory data processing agreement, in accordance with Norwegian legislation. When doing so, it is the data controller – meaning the individual enterprise – that is responsible for ensuring regulatory compliance. The agreement must clearly state where data is processed; this also applies to sub-contractors.[12] The agreement must not say anything to the effect that the provider (data processor) may use personal data for its own purposes, such as to improve its services.
- Enterprises must review their use of cloud computing regularly. This means that the enterprise itself, or a third party, must perform a security audit and ensure that the data processing agreement is being followed. In the event of an inspection, the enterprise must present an audit report to the Norwegian Data Protection Authority.
- The data controller must ensure that the cross-border transfer of data is in compliance with the law.
- Communication must be secure. Sensitive personal data must be encrypted.
- The cloud service provider (data processor) must keep personal data from different customers (data controllers) separate from each other.
- The solution used must be sufficiently documented, and the enterprise must be able to present documentation for inspection.

Procurement

Procurement of cloud computing differ in many aspects from traditional procurement processes in the public sector. Although the public procurement regulation does not in itself limit opportunities to procure or use cloud computing, there are many important aspects to take into consideration when procuring services like these:

Price comparisons

The purpose of regulations for public procurement is to ensure best possible use of society's resources. The cost of the procured goods or services throughout their life cycle is therefore important. This is often referred to as the *total cost of ownership* (TCO).

The TCO of running IT in-house can be calculated as the total of the costs for:[13]

- energy consumption (power to run the hardware, emergency power supply, power for cooling)
- employees (pay and social security costs)
- networks

[11] Norwegian Data Protection Authority: *En veiledning i bruk av skytjenester* [A Guide on the Use of Cloud Computing Services]

[12] This requirement follows from the Article 29 Working Party: *Opinion on C-SIG Code of Conduct on Cloud Computing.*

[13] The Scottish Government (2014): *Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector.*

- buildings (write-down, maintenance, rental, security measures, etc.)
- licences and maintenance agreements
- hardware

It is particularly relevant to take these into account when considering the cost of a service comprising a combination of, for example, Software as a Service that includes all the operating costs, compared with the cost of buying the software as a product and running it in-house or outsourcing it to a third party.

Requirements specification

To be sure of choosing the most advantageous offer, it is important to specify which functions are needed rather than presenting a detailed technical specification. This will reduce the risk of precluding some technology platforms right from the start.

Choice of contract

Customers can find it difficult to choose the right contract. Cloud services are often sold on standard terms and conditions that apply for all customers. Difi revised the Government Standard Terms and Conditions (SSA) in 2015, and the new agreements are better adapted to cloud services than the old ones, which drew a clear distinction between software and operation. The new SSAs allow the service provider's standard terms and conditions to be included. They can therefore be used for buying access to standard systems in the cloud. The SSA is then supplemented with the service provider's standard service agreement and, where appropriate, the data processing agreement based on the template produced by the Norwegian Data Protection Authority.

For more complex procurements, it can be difficult to align cloud services with the current standard agreements, which draw a distinction between procurement of software and hardware on the one hand[14] and procurement of operating services on the other.[15]

Exit costs

How does an enterprise retrieve its own data from the service provider if the customer relationship ends, regardless of reason? How can it move data to a new service provider? And what happens to data created as a result of operation, such as usage statistics? As when buying other software, it is important that enterprises avoid vendor lock-in or losing ownership of their own data. It is therefore important to ensure that they can retrieve their data in a reusable format. It is worth noting that the EU's new General Data Protection Regulation contains requirements for data portability. These apply to personal data but will in practice likely affect all types of data.

Most enterprises will need to store data over time, and it is therefore not unlikely that they will want to move data between service providers. It is particularly important for the public sector – which has an archiving obligation – to take into account their duty to preserve records for posterity. The archive creator has a duty to capture all digitally created archive material and to ensure that it is not lost if, for example, the enterprise changes service provider or if the service provider goes bankrupt.

---

[14] Difi: *Kjøpsavtalen* (SSA-K). [Sales and Purchase Agreement IT]. This agreement applies to procurements of IT equipment and/or software.

[15] Difi: *Driftsavtalen* (SSA-D). [Operational Services Agreement]. This agreement covers a wide range of operational services, focusing on standard services.

3 Cloud computing and legislative challenges

An interministerial working group has reviewed laws and regulations and assessed which legislation poses challenges for using cloud computing. The working group has also proposed possible amendments. The motivation behind this work has been to maintain protection of personal data, sound security, and preservation of important documents for posterity. The working group has weighed the intention of current legislation against today's technological reality, and has considered whether it is possible to uphold this intention and at the same time allow the potential of cloud technology to be exploited.

When current legislation is weighed against cloud computing, the main question that emerges is how to regulate *where* data can be stored. No existing regulations explicitly regulate the use of *technology* on which cloud services are based, but by setting requirements that data be stored inside a specific geographical area, laws and regulations can impose limits on use of the public cloud.

There are two important laws – in addition to the Security Act – that clearly impose requirements on where data must be stored: the Archives Act and the Bookkeeping Act.[16] The Personal Data Act also imposes requirements on data storage and processing, but these are less restrictive regarding which countries personal data may be stored or processed in.

Public Archives Act

Public bodies are obligated to hold archives that are designed in such a way as to ensure that documents be secured as information sources now and for posterity; cf. Public Archives Act, section 6. Public bodies must therefore set requirements to cloud service providers regarding availability, confidentiality and integrity (see chapter 4 for further discussion on the terms and conditions for use of cloud computing in the public sector).

Section 9(b) of the Public Archives Act states that archive material may not be *«sent out of the country».* Consequently, storage of archives in a cloud service using servers located outside Norway is in violation of the Act, even if an enterprise has deemed the nature of the archive content to be such that it can be stored abroad. The Director-General of the National Archives may give special consent to such storage. This follows from section 9(b) of the Public Archives Act.

The Public Archives Act and pertinent regulations do not regulate the use of cloud services for private individuals, organisations or enterprises. The Director-General of the National Archives may stipulate that private legal entities with public-sector affiliation comply with the Regulations relating to the Public Archives; cf. Public Archives Act, sections 19 and 20.

The Ministry of Culture has begun work on revising the Regulations pursuant to the Archives Act and will consider the need for amendments to the Public Archives Act. One of the intentions behind this work is to adapt archiving regulations to digitisation. In connection with

[16] Norwegian Ministry of Local Government and Modernisation (2015): *Kartlegging av hindringer i lovverket for bruk av skytjenester* [A survey of legal obstacles to using cloud computing services]. A report from an inter-ministerial working group with participation from: the Ministry of Finance, the Ministry of Justice and Public Security, the Ministry of Local Government and Modernisation, the Ministry of Culture, the Ministry of Education and Research, the Ministry of Trade, Industry and Fisheries and the Ministry of Transport and Communications.

this work, the ministry will consider the need for revision to allow public bodies to use cloud services with servers located outside Norway for archiving purposes.

The Director-General of the National Archives is also considering what requirements should be set in order to grant special consent to storing archives in cloud services located outside Norway. The Director-General of the National Archives aims to complete this work during spring 2016.

Bookkeeping Act

The Bookkeeping Act used to be one of the laws that posed the most obstacles to digitisation for business and industry because it restricted the physical storage of accounting records. Following its amendment, most accounting material may now be stored digitally. Because accounting and invoice processing are well suited as cloud services, requirements for storage of bookkeeping data deserve particular attention.

The current Bookkeeping Act states that enterprises with a bookkeeping obligation may *«store electronically accounting material in another EEA country if an agreement or pact with that country ensures Norwegian tax authorities satisfactory access to accounting information during the storage period and if such storage does not impede effective Norwegian police investigation».* The regulations pertaining to the act state that only the Nordic countries currently satisfy these requirements. Enterprises may therefore store their accounting data in a cloud service based in the Nordic countries, subject to notifying the Norwegian Tax Administration accordingly. It can be difficult to find public cloud service providers that can guarantee storage in the Nordic countries. This creates insecurity, particularly for small enterprises who know they can reduce their costs by using cloud services for accounting and invoice processing.

It is possible to apply for an exemption to store data in other countries. Such exemptions are regularly granted for storing information abroad as part of a common accounting solution within a group company or similar amalgamated entities. The condition is that they must have electronic access to the accounting data from Norway.

The purpose of the storage requirement is to give the Norwegian Tax Administration access to bookkeeping data for inspections. Accordingly, an enterprise wishing to use cloud services for processing or storing data outside the Nordic region may do so as long as a copy of the accounting data is transferred to Norway or another approved country as soon as possible and no later than seven months after the end of the financial year.

The Government will monitor future EU initiatives in this area and consider introducing measures that satisfy legal requirements to ensure Norwegian national authorities access to the information in such a way as to allow for storage in more countries than is allowed at present.

The EU and the Digital Single Market

Other countries have similar rules as Norway with regards to accounting data. In May 2015 the European Commission launched its *Digital Single Market (DSM) Strategy*. Initiatives to address restrictions on the free flow of data inside the EEA and unnecessary restrictions on data storage and processing represent a key element in the DSM strategy. Accounting and

bookkeeping data are identified as an area that often sets requirements for storage inside the respective countries.

Security Act

The purpose of the Security Act is to counteract threats against the sovereignty and security of the state and other vital national security interests. The Act should also help provide legal protection to individuals and ensure confidence in and control of the security services. The Act applies to administrative bodies and to enterprises supplying classified equipment and services to administrative bodies.

The requirements set out in the Security Act and Protection Instruction regulating how information systems are administrated make it inexpedient to store such information with foreign service providers. The Norwegian National Security Authority (NSM) is the only body that can approve and give permission to use such services for classified documents. NSM must approve all information systems that should process, store or transmit classified information. Electronic documents that are subject to the Protection Instruction must be processed in the same way as classified documents under the Security Act.

The Government has appointed a commission to propose a new legal basis for preventive national security (Security Commission). The recommendations put forward by the commission should ensure that new legislation takes into account technology developments, demographic developments and changes in the security situation. The commission will submit its report in autumn 2016.

Data protection and confidentiality

One area of uncertainty, though where regulations do not pose particular obstacles to using cloud services, is the storage of personal data. Nonetheless, regulation of this area sets important conditions for the use of services in the public cloud.

The Personal Data Act stipulates that personal data *«may only be transferred to countries which ensure an adequate level of protection of the data».* Consequently, personal data cannot simply be transferred to countries outside the EEA. However, some exceptions apply, one of them being that individual transfers may be approved in advance by the Norwegian Data Protection Authority, and provided the agreement with the data processor is based on the EU's model clauses, this will constitute a legal basis for transferring data. Moreover, some countries outside the EU, such as Canada, Australia and Switzerland, are already approved by the EU as secure recipient countries. Previously it was also permitted to transfer data to enterprises in the United States that were certified under the *Safe Harbour* scheme. The European Court of Justice declared the scheme invalid in autumn 2015, but a new scheme is expected to replace it: the *EU-US Privacy Shield* (see text box).

In the wake of this ruling, a number of considerations have had to be taken into account when entering into agreements involving the transfer of data to the United States. Until a new framework is in place, enterprises must use contracts that cover the EU's model clauses for personal data and notify the Norwegian Data Protection Authority.

Many enterprises wonder if they must take the Snowden revelations into account when considering the use of cloud computing. Despite the debate fuelled by Edward Snowden's

EU–US Privacy Shield

The EU–US Privacy Shield is a framework designed to protect the rights of EU citizens when personal data pertaining to them is transferred to enterprises in the United States. The new framework will place more stringent requirements on enterprises to protect personal data. Furthermore, US authorities will be required to monitor and enforce the framework.

There must be clear rules for and oversight of when US authorities may access data that is transferred to the United States under the new framework. This was one of the areas which, according to the European Court of Justice, was inadequately protected under the Safe Harbour framework.

Source: European Commission press release: *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, 2 February 2016.

disclosures, no changes have been made to Norwegian legislation or practice relating to the processing or storage of personal data or other data subject to confidentiality obligations. A country can determine its own regulations for how, for example, security authorities may gain access to data to combat terrorism or crime. Challenges arise when different countries making extensive use of data exchange have different views of what is acceptable when it comes to the right to monitor data and communication. These challenges need to be resolved at an international level.

New data protection regulation for the EU

For a long time now the EU has been working on introducing new legislation for processing personal data. The current Directive on Privacy and Electronic Communications applies inside the EEA. Because the Directive has been implemented in different ways in different countries, adapting to it proves difficult for enterprises operating in multiple countries, as cloud service providers often do.

Unlike a directive, a general data protection *regulation* would automatically become law in all EU member states, and likely also be incorporated into the EEA Agreement.

The EU member states have now reached agreement on the content of the new regulation. The issues in the regulation most relevant to cloud computing are presented below:

- Previously, the data controller was held responsible if data was lost, illegally accessed, etc. Under the new regulation, this responsibility will be shared between the data controller and the data processor. This means that more onus is placed on the cloud service provider as data processor.
- The right to transfer personal data between service providers will be established (the right to portability). In principle, this right applies to consumers, but since a growing number of service providers must develop mechanisms to manage this, it will likely also affect the commercial market.
- Customers – both consumers and enterprises (and any enterprise customers who are affected) – must be notified of data breaches or loss as soon as possible.
- Data may be transferred outside the EU provided the rules adopted by the European Commission are complied with.

- The regulation applies to all enterprises based in the EEA. It also applies for enterprises that process personal data pertaining to EEA citizens as the result of providing goods and services in the EEA, regardless of where those enterprises are based.
- It will become more important for all enterprises administrating personal data to comply with this legislation. Non-compliance with regulations may result in penalties of up to 4 per cent of worldwide turnover.

The regulation is expected to apply from 2018.

Duty of confidentiality

According to the Public Administration Act, any party who *«performs services or work for an administrative body»* is obligated to keep confidential all information concerning personal matters and business-related information that must be kept secret for competitive reasons. If a public sector enterprise enters into an agreement with a private company to process or store data, the duty of confidentiality will also apply to any employees in the company who are made privy to confidential information. It is important to ensure that the duty of confidentiality be incorporated into agreements with service providers who use subcontractors.

The eGovernment Regulations state that the risk of illegal access by means of electronic communications must *«be prevented in a satisfactory manner».* The Regulations also state that *«the administrative body must provide information about how confidential information and personal data are secured while being processed by the administrative body».* This applies to the use of ICT in general, not specifically to the use of cloud services.

Supervision

There is a need to oversee the ICT systems used by enterprises in many different sectors. Many supervisory authorities therefore conduct on-site supervision within their areas of responsibility. Enterprises using cloud services will find it difficult to meet supervisory requirements for physical control of their ICT systems. For example, most cloud service providers want to limit the number of persons admitted to their data centres because unauthorised persons pose a security threat.

Security requirements for ICT systems and infrastructure can also make it difficult for enterprises to decide whether or not to use cloud services. Statutory security requirements for ICT systems in different sectors are often complicated. For enterprises subject to regulations that apply in different sectors (such as enterprises providing both energy and communication services), the lack of harmonisation of requirements between sectors poses a challenge. This often emerges in connection with supervision and in the way in which supervisory authorities practice their respective regulations.

The Government will undertake a general examination of the supervisory function in multiple sectors in order to review issues relating to increased use of cloud services. On-site supervision, cross-border supervision, and system security requirements are issues which many supervisory authorities have to address and where there is a need to establish a common practice. A key question involves the use of third-party audits and how to ensure that enterprises conducting such audits are fully independent.

Measure: *Eliminate uncertainty caused by unclear legislation regarding the use of cloud services*

The Government will:

- Revise the Regulations pursuant to the Public Archives Act and, where appropriate, the Public Archives Act, to better adapt archiving regulations to digitisation. Among other things, it will consider the need for revision to allow public bodies to use cloud services with servers located outside Norway for archiving purposes.
- Assess the possibilities for expanding the number of countries where bookkeeping data can be stored legally outside Norway. Important measures in this area are already under way in the EU, and Norway will monitor developments closely.
- Harmonise supervisory practices as far as possible, so that enterprises do not encounter conflicting requirements regarding cloud computing from different supervisory authorities.
- Contribute to the EU's work on establishing common criteria (standards, certification schemes, etc.) for cloud computing.

4 Conditions for using cloud computing in the public sector

Many enterprises are uncertain about the legal framework conditions governing the use of cloud computing.[17] The review of the legislation in chapter 3 shows that there is considerable scope for the lawful use of cloud services by enterprises in Norway – including those in the public sector.

Principles for using cloud computing

In addition to the need for legislative clarification, the ICT industry and public sector enterprises are also calling for clear guidelines from central government regarding the use of cloud computing.

The Government has therefore established some principles for the use of cloud services in the public sector:

- *Cloud computing shall be assessed on the same basis as other solutions when considering major changes or reorganisation of ICT systems or operations:*
  - *when procuring systems or major upgrades*
  - *when undertaking extensive replacements of hardware*
  - *when existing operating agreements expire*
- *When they offer the most appropriate and cost-effective solution and when no particular obstacles stand in the way of using them, cloud services should be chosen.*
- *The chosen solution must satisfy the agency's requirements for information security. This means that enterprises must know the value of their own systems and data, and perform a risk assessment of the chosen solution.*

Although cloud services may offer several advantages, they may not always be the best solution. Several factors may make other development or operating solutions better suited to meeting the needs of an enterprise, such as special requirements for national security, or if cloud services would not prove cost-effective given the enterprise's current systems and infrastructure. The Government will therefore not establish a *cloud first* policy; however, the principles will help ensure that cloud services are considered when public agencies need to procure new ICT systems or operating solutions.

The principles for using cloud services were included in the Circular on Digitisation for 2016. The Circular on Digitisation presents an overview of orders and recommendations for digitisation that apply to all ministries, regular government administrative bodies, administrative bodies with special authority and government administrative enterprises.

The Circular on Digitisation sets out requirements for architecture and standards for public agencies.

[17] Nexia Management Consulting (2015): *Kartlegging og analyse av landskapet for offentlige datasenter i Norge* [A survey and analysis of the landscape for public data centres in Norway]. Prepared for the Ministry of Local Government and Modernisation, June 2015

Although municipalities and counties are not included in the circular, the principles give an important signal to them, too, and they may of course choose to follow the principles if they so wish.

The principles will be followed up with support, guidelines and tools in order to aid public sector organisations with the procurement of cloud services.

The need for guidance and control

The public sector has a particular need to ensure control over who manages information and where this is done. The form and degree of control required will depend on the type of information processed by the respective organisations. A range of control mechanisms are available:

Contracts
If needed, a contract can stipulate specific requirements for data processing and storage. A standard contract from the service provider could well be used, provided it guaranteed the use of specific technologies or standards, or met requirements for specific certifications in such a way as to satisfy the requirements imposed on public sector enterprises. Mechanisms for revision and contract management could also be negotiated, if specific needs warranted it.

Prequalification of service providers
Service providers could prequalify for processing specific types of information, either generally or for specific sectors. The Ministry of Local Government and Modernisation will assess whether it is possible and desirable to establish a marketplace for cloud services for use in the public sector in Norway. Such a marketplace could serve as a form of prequalification of service providers. In the UK G-cloud, companies can be accredited for managing data requiring a specific security level.[18]

Entering into common agreements on behalf of the public sector
The state could enter into agreements with suppliers of data centres/cloud services on behalf of the public sector. Such agreements could be put out to tender in the market and contain requirements that satisfied the needs of agencies with the most stringent security requirements for processing and storing information. This is also a form of contractual control, but the contract would be negotiated and monitored by central authorities rather than by individual organisations.

Designated data centres for government agencies or the public sector
Central government could establish one or multiple data centres that satisfied the most stringent security requirements, for use either by central government agencies or by the entire public sector.

Through various meetings and activities, the Ministry of Local Government and Modernisation has mapped the need for control associated with cloud services and ICT operation in the public sector. This work involved examining the landscape for public data centres in Norway along with the futures plans and needs of public sector enterprises.[19]

---

[18] Cabinet office (2013): *G-Cloud or PSN Service Description and Commitment for Security Accreditation*. Version 4.04.

[19] Nexia Management Consulting (2015): *Kartlegging og analyse av landskapet for offentlige datasenter i Norge* [A survey and analysis of the landscape for public data centres in Norway]. Prepared for the Norwegian Ministry of Local Government and Modernisation, June 2015.

Central government agencies and municipalities and county municipalities have been involved in this work. Through these activities, a no need was identified for central government to negotiate common operating agreements on data centres or to establish a common data centre specifically for central government agencies or public sector enterprises. These alternatives are therefore not discussed further in the strategy.

The investigations conducted by the Ministry of Local Government and Modernisation clearly revealed that what public sector enterprises needed most was guidance from central government to ensure good procurement practices and that the contracts they enter into are balanced, and satisfy Norwegian regulations. The enterprises also indicated that procuring cloud services would be simpler and more secure if some form of prequalification, approval or accreditation of suppliers were in place.

The Government wants to set up mechanisms to help public sector enterprises make sure that they have the necessary control through sound procurement practices and contracts that satisfy government requirements, and through contract management. As a starting point, entering into contracts that satisfy the identified requirements, and ensuring proper contract management, ought to offer sufficient control to public sector enterprises not subject to the Security Act.

Contractual control

Contracts and agreements constitute the key mechanism for regulating the relationship between customer and supplier. In the consumer market, a long-standing challenge has been that end-user licence agreements are long and difficult to understand, and often set unreasonable terms. The consumer has no influence over the content of such agreements.

The situation in the corporate market is more nuanced. Although standard agreements are used there, too, since standardised services and purchasing processes help make cloud services affordable, the tendency has been towards more balanced agreements than in the consumer market. This is partly the result of increasingly stringent government requirements and more informed customers. The best for all parties would be to use standard agreements that also satisfy customers' requirements. To realise this, it is vital that public authorities – preferably at European level – reach agreement on common requirements. Such requirements could either be cross-sectoral or sector-specific. Norway's early adoption of technology in many areas puts us in a favourable position in terms of influencing suppliers who are keen to win reference customers in the public sector. At the same time, it is important that Norway also works actively with the EU on establishing common standards and requirements.

Cloud service procurements are poorly suited to standardised frameworks such as the Government Standard Terms and Conditions (SSA). It will therefore be important to establish checklists to enable public sector enterprises to ensure that their supplier's standard agreements do not violate Norwegian regulations and that they cover the same areas as in the government standard terms and conditions. Developing such checklists will form part of the guidance work performed by the Agency for Public Management and eGovernment (Difi).

It is of course possible for public sector enterprises to use cloud computing even if they have specific requirements and need to negotiate specific terms and conditions. In such cases, the process of purchasing cloud services will be more like the traditional procurement process.

Regardless of whether a standard agreement is used or special terms are negotiated, it is important to make sure that mechanisms for contract management are in place. One such mechanism could be to have an independent third party perform audits to check that suppliers honour their contractual obligations. It is important to make sure that such third parties are fully independent of the supplier.

Guidance from the Agency for Public Management and eGovernment (Difi)

The Ministry of Local Government and Modernisation will charge Difi with the task of establishing a team of experts and an online resource where public sector enterprises can seek guidance on cloud computing. In the long term, the guidance would ideally be adapted to different target groups with similar requirements and needs and to sector-specific needs.

Such a resource must cover all the stages in the procurement process, and not only the legal issues associated with the procurement itself. Relevant issues and tasks could be:

- How to conduct the procurement process correctly when a cloud service is considered the best option.
- Risk assessments adapted to the complexity and needs of different types of enterprises, ideally with examples of best practice.
- Requirements for data processing agreements.
- Templates and guidelines for setting up a cost-benefit analysis for using cloud services.
- Best practice for chosen solutions, ideally with examples from different types of representative enterprises, such as primary and lower secondary schools, municipal administrations or general practitioner clinics.
- How to ensure contract management through, for example, supervision and independent third-party audits.

Difi's service will be directed at public sector enterprises – including municipalities – but will also be relevant to suppliers to the public sector. However, there is a clear need for this type of resource in business and industry, particularly for small and medium-sized enterprises. Difi's resources for the public sector could serve as a model for a similar service directed at business and industry; for example, under the auspices of one or multiple industry organisations.

Sectoral information value assessment

Public information can be divided into three categories:[20]

1. information that should only be stored in Norway
2. information that can be stored abroad but that can be returned to Norway if necessary, subject to specific conditions
3. information that can be stored abroad without being subject to specific conditions

The individual sectors are best qualified to evaluate in which category their information belongs. Many sectors have already begun work on assessing their requirements for using cloud computing or on developing guidelines for their sectors. The Government will ask all

[20] NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden* [Digital Vulnerability and a Secure Society: Protecting Individuals and Society in a Digitised World].

sectoral authorities to prepare assessments of the information in their respective sectors and of how it can be processed using cloud computing.

The Personal Data Act will likely determine how some sectors categorise their information. Personal data will fall under category 2 or category 3, provided EU requirements for transfers of personal data abroad are satisfied. The Norwegian Data Protection Authority has prepared useful guides on the storage and processing of personal data in cloud computing. Other sectors may have to take into consideration sector-specific regulations, such as the Health Registries Act or the Regulation on Emergency Preparedness. These sectors must conduct their own analyses based on their particular information and needs. Such analyses must consider what circumstances might require information to be returned to Norway, how it could be regulated in contracts with suppliers, and how it would be achieved in practice.

Sensitive information is probably the most important type of information that will fall under category 1, though some sectors or enterprises may well consider other types of information to be so critical that storage in Norway is seen as the only option.

It is important that public sector enterprises seeking guidance have an authoritative resource where they can be sure that the information on data classification is up to date and correct, regardless of sector. Difi's task will therefore also entail coordinating and harmonising the work of the respective sectors. This work should be conducted in close cooperation with the Norwegian National Security Authority.

Certification requirements

A wide range of certification schemes relevant to cloud services are available. Many suppliers also choose to follow requirements issued by the EU or individual countries. Some examples of such requirements are:

- international standards, such as ISO 27001
- requirements issued by national authorities, the EU's model clauses or the EU–US Privacy Shield
- standards that are not international but that have been accepted as de facto standards in their respective areas, such as FedRAMP, SOC, UK G-Cloud and Singapore MTCS
- standards associated with specific sectors, such as HIPAA (health), FISC (finance) and PCI DSS (payment cards)

The leading cloud service providers, such as Google, Amazon and Microsoft, hold most of the certifications. Smaller providers often select certifications that are relevant to their specific sector or to the markets at which their services are targeted. Obtaining certifications in many areas – and maintaining them – is a costly process for small service providers. Universal agreement on a smaller set of standards that cover the main areas of cloud computing would be seen as beneficial.

We know that common EU requirements – such as for processing personal data or for security certification – often prompt cloud service providers to adapt their services and standard agreements to meet such requirements. This makes it easier for enterprises to assess the services available. The Government therefore wants to contribute to EU efforts to implement common criteria for cloud services at different levels.

Examples of standards and certifications

ISO 27001:	ISO 27001:2013 specifies requirements for information security management systems. This standard forms the basis for most certification schemes.
ISO 27018:	ISO 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
SOC1, SOC2, SOC3:	Service Organization Control reports. Reports developed by the American Institute of Certified Public Accountants (AICPA). SOC1 reports on financial data. SOC2 reports on control mechanisms more specific to data storage and processing, such as security, accessibility, processing integrity, confidentiality and data protection. SOC3 covers the same elements as SOC2 but on a higher, less technical level.
FedRAMP:	Federal Risk and Authorization Management Program. A standardised approach to verification of security, authorisation and monitoring for cloud services used by federal agencies in the United States.
UK G-Cloud:	Enterprises seeking high-level security accreditation in the UK framework, G-Cloud, can apply for this. The National Technical Authority for Information Assurance (CESG) is the accrediting body.
MTCS:	Multi-Tier Cloud Security. From Singapore. An open certification scheme for cloud service providers, based on ISO 27001. Three levels of security certification (Tiers 1 to 3) meet stringent information security requirements. Certification is performed by independent certifying bodies such as DNV-GL and the British Standards Institution (BSI).
HIPAA:	Health Insurance Portability and Accountability Act. US law regulating the processing of patient information. An independent third party checks that the data processor complies with the law.
FISC:	Center for Financial Industry Information Systems. From Japan. Security guidelines for financial information systems.
PCI DSS:	Payment Card Industry Data Security Standard. Global certification standard for organisations processing payment card transactions.

The Government also wants to require service providers to the public sector in Norway to hold certifications or to be able to document that they meet the standards that are set for the sectors they serve. Where relevant, each sector must determine which standards or certifications should apply in their area. Difi has responsibility for coordinating this work.

Example: UK G-Cloud – Digital Marketplace

G-Cloud is a framework for procurement of cloud computing services aimed at the public sector in the UK. The framework opens for supplier applications at regular intervals (every 6 to 9 months).

Suppliers register details about their company, what services they provide, and price information on a dedicated website. The services must satisfy the NIST definition of cloud computing. Suppliers also register information about themselves and how their service is delivered, their approved security level, etc. Registration is largely based on self-declaration.

Public sector enterprises can use the Digital Marketplace to search for suppliers. They can request more information if, for example, they have special security requirements. They can also select suppliers directly without going through the traditional procurement process. The UK authorities regard the conditions for public procurements to be satisfied by announcing registration in the framework. The prices stated in the framework are transparent, so suppliers may amend their prices to become more competitive.

An important idea behind G-Cloud and Digital Marketplace is that it should be easier for small and medium-sized companies to compete for public-sector contracts.

Source: UK Cabinet Office – Government Digital Service.

A marketplace for cloud services aimed at the public sector

The Government wants to see a form of prequalification and/or accreditation scheme established for cloud service providers. The Ministry of Local Government and Modernisation will investigate potential models for a marketplace for cloud services aimed at the public sector and consider possible implementation in Norway. Such a marketplace would provide a measure that would make it easier for enterprises to assess cloud services as an alternative when procuring new ICT systems and may include mechanisms for self-declaration, prequalification and/or accreditation for different security levels. The investigation with be carried out in 2016.

Coordinating the establishment of new data centres

Agencies or sectors who define their information to fall under category 1 (information that should be only be stored in Norway) may well want to establish a dedicated data centre or possibly buy services from a (Norwegian) provider who can deliver high-security services.

In such cases, the Government wants to facilitate better utilisation of existing data centre resources in the public sector. Government agencies requiring high-security services must consider the possibility of utilising free capacity from – or cooperating with – other agencies with similar needs. This requires gaining an overview of the organisation and capacity of public data centres, first and foremost in central government agencies. Difi will have responsibility for implementing such a system.

Example: Skyscape

Actors in the UK market have set up a data centre that meets the needs of public agencies with particularly stringent security requirements. *Skyscape* is a provider of infrastructure services (IaaS) in the UK G-Cloud procurement framework. Skyscape consists of an alliance of different suppliers: the partly state-owned defence technology company QinetiQ, VMWare, Cisco, EMC and Ark Data Centres. The company's data centres and cloud services are accredited by the UK authorities for data classified up to OFFICIAL-SENSITIVE. Skyscape is also accredited by the *Health and Social Care Information Centre* (HSCIC) for supplying services to the National Health Service.

Skyscape is generally not used by public agencies with low security requirements. For example, the UK's HM Revenues & Customs (HMRC) has chosen Google Apps in a cloud solution for office support. Under the agreement, it is accepted that data can be stored in Google's data centres located outside the UK.

Sources: Skyscapecloud.com, digi.no, Financial Times

Systems that process classified and sensitive information, including electronic documents subject to the Protection Instruction, must in principle be located in Norway. Enterprises who are subject to the Security Act would have to make special assessments if they wanted to use services in the public cloud. In such cases they should consult the Norwegian National Security Authority.

Measure: *Make it easier for public and private enterprises to consider cloud computing as an alternative when procuring new ICT services*

The Government will:

- Establish resources to support agencies in assessing and procuring cloud services:
  - In the short term, existing material will be collated and adapted to provide guidance on cloud service procurements.
  - In the long term, a more comprehensive resource will be established to provide guidance on cloud service procurements in the public sector. Important areas where guidance is needed are: information value assessment, risk assessment, and information security. This work must be coordinated with the sectors' own assessments of information and development of guidance material.
  - This resource will make recommendations for certifications or standards which cloud service providers targeting given sectors should satisfy. Each sector must determine which standards or certifications should apply in their area.
  - It is natural for such a resource to be established under the auspices of the Agency for Public Management and eGovernment (Difi) and that the work be incorporated into the ICT procurement guidance service provided by Difi. The expert resource will initiate cooperation with relevant industry organisations so that they – should they so wish – can use Difi's resources to provide guidance to their members.
- Charge the Ministry of Local Government and Modernisation with examining and assessing different models for a potential marketplace/procurement framework for cloud services aimed at the public sector.
- Facilitate better utilisation of existing public data centre resources for agencies with a need for such stringent controls that they are considering buying high-security services or establishing their own data centres in Norway. In such cases, agencies must assess the possibility of utilising free capacity from – or cooperating with – other agencies with similar needs. This requires gaining an overview of the organisation and capacity of existing data centres, first and foremost in the public sector. Difi will have responsibility for implementing such a system.

Published by: Norwegian Ministry of Local Government and Modernisation

Publication number: H-2365 E

Cover photo: Jan Hausken/KMD
Print: Norwegian Government Service and Security Organisation 06/2016