A guide to
CLOUD COMPUTING
2014

Datatilsynet

Cloud computing

Businesses that make use of cloud computing are legally liable, and must ensure that personal data is processed in accordance with the relevant legislation and regulations.

If you, as a private individual, are going to use this type of online storage solution, you should consider carefully how secure the system is.

Contents

What is cloud computing?

Cloud computing is the collective term for everything ranging from data processing and storage to software available online from third-party server parks.

Characteristic of server parks is that they are built to be dynamically scalable. This means that computing power can be adapted to capacity requirements, with the customer paying only for the services actually used.

Many third-party server parks are located outside Norway. A major challenge for businesses using these services is to ensure that the agreement with the cloud service provider complies with Norwegian law.

Various forms of cloud computing

Cloud computing is normally divided into service models, the three most common of which are:

- Software as a Service (SaaS), where the customer uses the vendor's application(s) over the internet by means of a cloud network infrastructure. In principle, the customer has no control over the applications, networks, servers, operating systems or storage devices.
- Platform as a Service (PaaS), where the customer installs applications developed/ purchased by the customer in the vendor's cloud network infrastructure by means of a programming language and tools supported by the vendor. The customer has control over his own applications, but not over networks, servers, operating systems or storage devices.
- Infrastructure as a Service (IaaS), which applies to the provision of computer infrastructures as a service over the internet. The customer has control of relevant applications, servers, operating systems and storage devices, as well, in some cases, as certain elements of the network (such as firewalls).

Cloud services can be divided into delivery models, such as:

- Public cloud, where the vendor makes cloud computing services available to all customers.
- Private cloud, where cloud computing services are made available only to those businesses to which they apply. Here, the environment(s) that the cloud services are delivered from will typically be dedicated to the individual customer or a defined group of customers. This arrangement enables a greater level of customisation than is possible in the public cloud model.
- Hybrid cloud, which can be a combination of the models described above.

The enterprise is liable as data controller

Providers of electronic services on the internet are bound by the same rules regarding the *processing of personal data* and the responsibilities of the data processor as more traditional businesses. Data processing is defined in Section 2(2) of the Personal Data Act.

The data controller decides whether cloud computing services should be used. If a service processes data on behalf of the data controller, the service provider is deemed to be the *data processor*. The Norwegian Data Protection Authority therefore considers providers of cloud services to be data processors, irrespective of the service provided.

Data controller

The data controller is the person or entity that determines the purpose for which personal data is to be processed and the means to be used therefor. This is normally an enterprise.

A data processor cannot process personal data in any other way than that agreed with the data controller, see s 15 of the Personal Data Act. The data processor also has a duty to perform security measures in accordance with s 13 of the Personal Data Act and Chapter 2 of the Personal Data Regulations. A data processor agreement does not exempt the data controller from their statutory liability.

The Norwegian Data Protection Authority has prepared a guide for drawing up such a data processor agreement, as well as a draft example. These can be found at datatilsynet.no. The draft agreement and guide also contain a list of minimum requirements that the Norwegian Data Protection Authority expects such an agreement to contain.

The actual agreement may encompass other issues, but this will depend on the internal control procedures of the data controller purchasing the service. Such issues might include backup copying, deletion, access management and the segmenting of databases.

Internal control

A well-functioning internal control system is crucial to ensuring that personal data are processed in the proper manner. The Norwegian Data Protection Authority has prepared a guide to internal control and data security, which is available from datatilsynet.no. The guide helps the enterprise through the process of introducing internal control and data security measures. In the following, we will discuss some of the key routines that need to be put in place before cloud computing is implemented.

Identify the enterprise's data processing activities

The enterprise must identify which personal data processing activities are undertaken, and which personal data are included in each process. This overview is necessary if the enterprise is to fulfil its obligations. It also forms the basis for the enterprise's security strategy and objectives, and will underpin all its risk assessments.

What the overview should contain

The overview should give brief details of:

- which data are processed and why.
- the authority under which the data are processed.
- how the personal data are classified – are they sensitive or not?
- technical security measures, indicating zones or networks.
- where the data are stored and whether they are transferred via external media.
- the scope of the personal data.
- any departments that process the personal data.
- system owners and/or data owners.

Routines for internal control

The enterprise must have internal control routines in place. Some of the most relevant routines cover:

- access
- correction and addition
- deletion
- information
- consent

More detailed information about routines and how to develop them can be found in the guide to internal control and data security at datatilsynet.no.

Please note that the same duties apply to data controllers irrespective of whether they use cloud computing or not.

Risk assessment and data security

The enterprise must perform a risk assessment in connection with changes in factors which could affect data security, e.g. changes in the information system or in the threat landscape. Risk describes the relationship between the likelihood that an unwanted incident may occur and the consequences such an incident would entail. The risk assessment must be seen in the context of established risk acceptance criteria, and the data controller must implement the measures necessary to achieve a satisfactory level of data security.

To achieve a satisfactory level of data security, the data controller must ensure that any cloud computing service meets the requirements specified in the acceptance criteria and risk assessment. The enterprise must accord the assessment greater weight when it switches from in-house operations to cloud-based solutions, since the personal data will lie outside the data controller's direct control. The question is: How can the data controller ensure that the level of data security is adequate?

The data processor agreement must contain a section relating to data security, and it is important that the data controller reviews this thoroughly. The agreement in itself is no guarantee that the service provider has a satisfactory level of data security.

Security audits

Chapter 2 of the Personal Data Regulations, which deals with data security, contains a provision relating to security audits:

"Security audits of the information system's use shall be carried out regularly. A security audit shall comprise an assessment of organisation, security measures and use of communication partners and service providers. If the security audit reveals any unforeseen use of the information system, this shall be treated as a discrepancy, see s 2-6. The result of the security audit shall be documented."

The Norwegian Data Protection Authority is therefore of the opinion that:

- The data processor must be able to document the information system's design and security solutions. This is to enable the data controller to make sure that the solution affords adequate data security in relation to the risk assessment and acceptance criteria.
- The data processor cannot change the data security measures without the data controller having been notified in writing of and consenting to the change.

Read more about data security and internal control at datatilsynet.no.

Special issues

In principle, providers of cloud computing services enjoy some advantages over providers of traditional server services. For example, cloud-based services offer more flexibility and integrated solutions. However, such advantages also raise some special issues, which the data controller must address:

Backup copying/mirroring: How does this work? Are personal data transferred to another country for redundancy, e.g. from Ireland to the USA or from Germany to India? Is such redundancy in accordance with the agreements that have been entered into? How are the personal data processed after they have been transferred?

Segmenting: The Norwegian Data Protection Authority has stated that the data controller's personal data must not be mixed with personal data from another *data controller*. How does the service provider handle this issue?

Access management: Which of the service provider's staff have access to the personal data being processed? Do the access management controls comply with statutory requirements and the vendor's own internal control systems? See also the section on risk assessment and data security.

Authorised and unauthorised use: Does the solution permit the logging of authorised and unauthorised use, pursuant to Section 2-14 of the Personal Data Regulations?

Documentation: Is the solution adequately documented with regard to controls by public authorities?

Where is data stored? Transfer to a third country: In principle, personal data may not be transferred to countries outside the EEA. However, one-off transfers may be approved in advance by the Norwegian Data Protection Authority. In addition, certain countries have been approved by the EU as safe receiving states. Enterprises that wish to transfer personal data abroad must comply with the provisions of Chapter 5 of the Personal Data Act and Chapter 6 of the Personal Data Regulations.

Deletion: Are personal data deleted within a "reasonable time"? The data processor has no right to process personal data after being asked to delete them by the data controller.

Use for own purposes: Does the data processor have a clause in the agreement entitling them to use data for their own purposes (e.g. to improve their own services)? The enterprise must ensure that the data processor agreement carries more weight than any other, and that the service provider does not have a privacy waiver that can supersede this. The data controller must ensure that the personal data being processed are used only for explicitly stated purposes that are legitimately justified by the activities of the data controller, as stipulated in Section 11(b) of the Personal Data Act.

Subcontractors: Does the data processor make use of subcontractors? The identities of any subcontractors must be known to and approved by the enterprise. This relates to the issue discussed above concerning where data are stored and whether they are transferred to a third country.

Checklist

Perform a risk assessment and threat analysis

- Identify all the enterprise's systems containing personal data. Then grade the data from sensitive to non-sensitive.
- Evaluate what could go wrong.
- Assess the consequences if anything were to go wrong, e.g. that personal data falls into the wrong hands.
- Create a list of security measures that have been implemented to deal with any incidents.
- Assess the security measures in the agreement with the cloud computing service provider. Does the service meet the requirements identified in the risk assessment?

Make sure you have a data processor agreement with the provider of any cloud computing services

You have a duty to enter into a data processor agreement with the provider of any cloud computing services. You must ensure that this complies with Norwegian law and regulations. It is the responsibility of the enterprise to ensure the statutory requirements are at all times complied with. Important issues that must be covered in the agreement include: backup copying, deletion, access management and data segmentation.

- How does backup copying/mirroring work?
- When are data held by the service provider deleted?
- Is access management in accordance with statutory requirements and the service provider's own internal control systems?
- How does the service provider ensure that personal data from one data controller is not mixed with those of another?
- Find out whether the service provider can use the enterprise's data for its own purposes.
- Ensure that the service provider's privacy terms (or other terms) do not exceed the provisions of the data processor agreement.
- Make sure you regulate the service provider's use of subcontractors, and that the enterprise has an overview of and control over such subcontractors.

Audit the data processor

- The use of cloud computing services must be audited on a regular basis. In other words, you yourself or an independent third party must perform a security audit to ensure that the data processor agreement is being complied with.
- If the agreement states that a third party is to perform the audits – ask to see the final audit report. This report must also be made available to the Norwegian Data Protection Authority if we ask to see it during one of our inspections.

Make sure that any transfer of data is lawful

- Transfer to a third country: In principle, personal data may not be transferred to countries outside the EEA. However, the Norwegian Data Protection Authority may authorise such transfers in advance. In addition, certain countries have been approved by the EU as safe receiving states.

Portability of data

- Can the data be transferred to a new service provider if this is deemed desirable?

Ensure secure communication and encryption

- Are data encrypted before they are stored in the cloud?
- Is communication between the data controller and the data processor encrypted?
- Is communication between the data processor and any subcontractors/data centres encrypted?
- Who holds the encryption keys?

Put the necessary documentation in place

- Is the solution adequately documented, so that public authorities can perform an audit?

Private use of cloud computing services

If, as a private individual, you are going to use cloud-based data storage solutions, you should ask yourself the following questions:

User terms and conditions: What do the user terms and conditions say? Should I be worried about any of them? Do I understand them?

Reliability: How reliable does the service provider seem? Do I know anyone who can advise me on whether the service is appropriate for my purposes?

Security: How well does the service provider seem to handle the issue of security? How easy does it look for unauthorised individuals to gain access to the system? Will the data I want to store be adequately secured? It is a good idea to seek the advice of others who are knowledgeable about security.

Password: It is a good sign if the service provider sets a standard for the quality of any passwords. Does it seem as though the service provider is handling this in a good way?

Rights: What rights do I have if all the data I have stored with the service are lost? Do the terms and conditions say anything about this? Do I have my own backup copy?

Legislation: Which country is the service based in? Who can help me if anything should go wrong? In principle, with cloud-based solutions the data could be stored anywhere in the world, and the rules applicable abroad may be different to those that apply in Norway.

Further reading

From the Norwegian context

Can we use cloud computing services? Privacy blog, 13 October 2015: (in Norwegian)

The cloud computing strategy for Norway

European and international guidelines

European Article 29 Working Party and the international Berlin Group's assessments of cloud computing.

Working paper on cloud computing from the Berlin group (pdf)

The EU's Recommendations on Cloud Computing and Safe Harbor

Code of conduct

At the European level there is a working group called the Cloud Select Industry Group (C-SIG) which, together with the European Commission, is working on a Code of Conduct for providers of cloud computing services. This will involve service providers having a uniform practice with regard to compliance with privacy regulations in Europe. The Article 29 Working Party will then determine whether this Code of Conduct is sufficient to address the uncertainties and issues which have been practised over a long period. So far, the Article 29 Working Party has not approved this Code of Conduct, but it has issued a statement on what elements must be included before it can be approved.

The Article 29 Working Party's statement on C-SIG Code of Conduct on Cloud Computing

Public sector use of cloud services

In 2012, the Norwegian Data Protection Authority gave the go ahead for the municipal authorities in Moss and Narvik to start using cloud computing services from Google and Microsoft.

Read the decision here

Office address:
Tollbugata 3, 0152 Oslo

Postal address:
PO Box 8177 Dep, 0034 Oslo

postkasse@datatilsynet.no
Tel: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no