Nordic Council of Ministers

Ved Stranden 18
DK-1061 Copenhagen K

www.norden.org

NORDISKE ARBEJDSPAPIRER
NORDIC WORKING PAPERS

Legal guide to public cloud sourcing

Nordisk Ministerråds uformelle forum for IT-direktører

http://dx.doi.org/10.6027/NA2013-933
NA2013:933

This working paper has been published with financial support from the Nordic Council of Ministers. However, the contents of this working paper do not necessarily reflect the views, policies or recommendations of the Nordic Council of Ministers.

Legal guide to public organisation cloud sourcing in the Nordic countries

Nordic Council of Ministers' informal forum for IT directors

17. December 2013

Content

Legal guide to public organisation cloud sourcing in the Nordic countries

Scope

The aim of this guideline is to provide a practical tool for public organization buyers in the Nordic countries to ensure legal compliance, contractual efficiency and proper handling of risks and selection of safety measures in situations where the organisation is contemplating to cloud source certain IT services. On behalf of the Nordic Council of Ministers' informal forum for IT directors, this guideline has been drafted by Deloitte and completed in cooperation between different Nordic authorities.

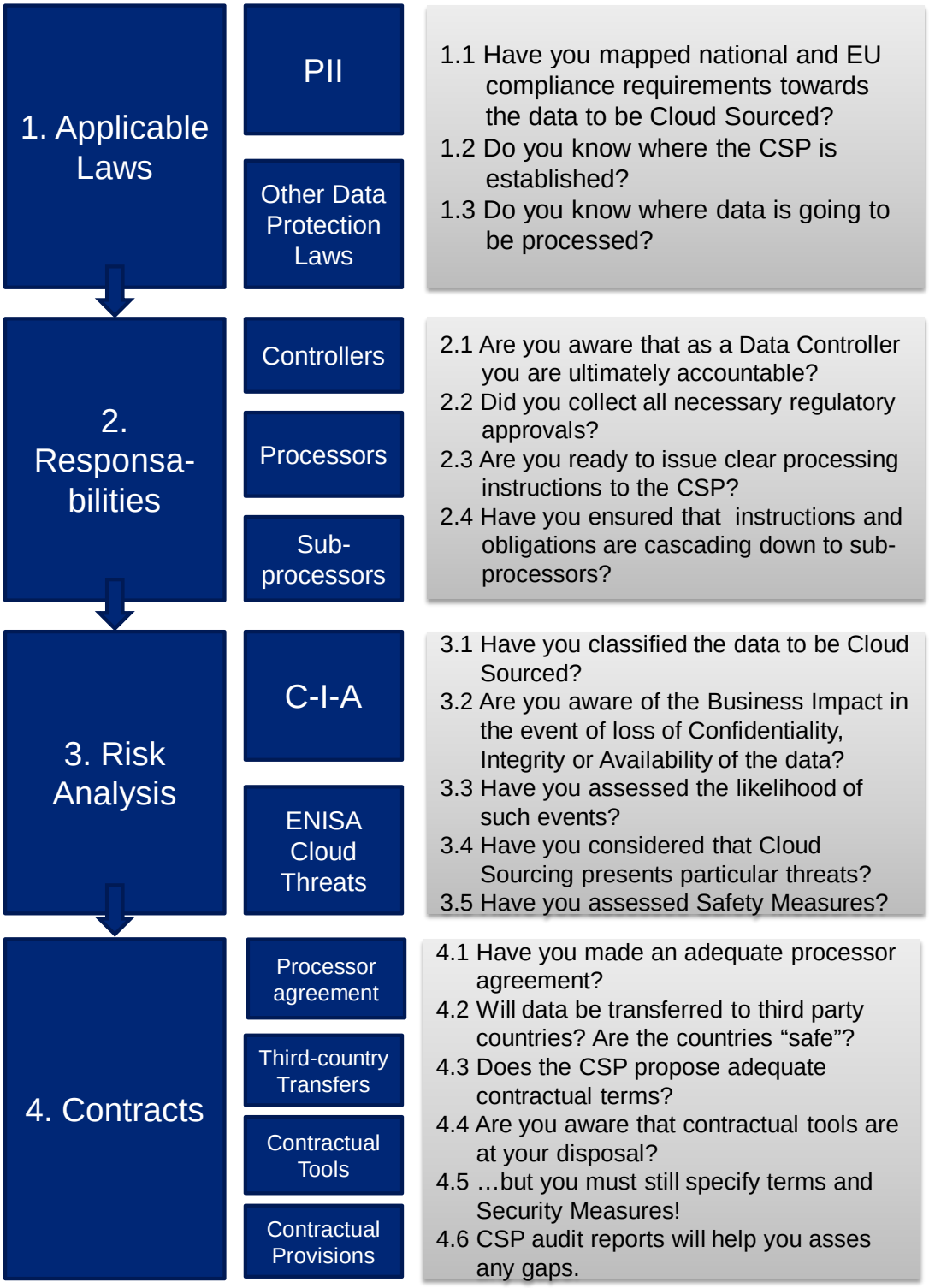
The guideline will primarily focus on the case of cloud sourcing of IT services in which Personal data is processed, as this is one of the most common scenarios in the context of public organisations. Moreover, many sources of interpretation concerning legal requirements, contractual tools, handling of risk, etc. are available on this particular subject matter.

The reader should keep in mind that cloud sourcing of other types of data than personal data can also result in risks and/or requirements that the organisation would have to handle. Many of the guidelines' advice are equally applicable outside the personal data use-case.

The EU directive 95/46/EC on Data Protection is the legal framework of the guideline. The guideline is primarily based on the EU Article 29 Working Party's opinion of 05/2012 on cloud computing, ENISA's published reports, the EU directive 95/46/EC on data protection and other such sources that contribute to ensure a common best practice on the subject of cloud sourcing in Europe. The guideline strives to describe a uniform approach and should therefore be useful to all the Nordic countries in spite of differences in the national legislations.

The guideline does not intend to describe the complete legal framework around the processing of personal data, but instead tries to cover the most common points of attention with regard to cloud sourcing and to show the steps of a reasonable due diligence process.

The guideline will address the following topics and key issues:



The figure above shows the four key topics in chronological order on the left side of the figure: Applicable Laws, Responsibilities, Risk Analysis and Contracts. For each topic a number of key issues have been identified in the second column. The third column is a practical checklist, covering the main questions and attention points organisations should focus on when choosing to cloud source certain IT services.

Definitions and terminology

Below are definitions of the roles and terms that are used in this guideline.

Public organisations
We use the term public organisation (or "organisation") for state sector organisations plus organisations of local government. For the purpose of this guide they will coincide with the data controller.

Personal data
The term personal data refers to data relating to an individual who is or can be identified, either from the data or from the data combined with other information that is likely to be included in the processing.

Sensitive personal data
Sensitive personal data includes data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life. Data relating to offences, criminal convictions or security measures as well as data relating to administrative sanctions or rulings in civil cases shall also be handled as sensitive data.

Data Protection Agency/Authority (DPA)
A DPA is a governmental authority charged with data protection tasks: issuing acts of regulation, issuing administrative decisions in data protection matters, incident monitoring, awareness, acting as custodian for declarations, etc. The exact prerogatives of the DPA can vary from country to country.

Data processing
Data processing is defined as any operation or set of operations which is performed upon personal data, either by manual or automatic means.

Data controller
The natural or legal person, public organisation, agency or any other body which determines the purpose or means of the processing of the personal data. In this guideline this would be the public organisation that wishes to outsource a data processing service to a CSP.

Data processor
The natural or legal person, public organisation, agency or any other body who processes the personal data on behalf of the controller. In this guideline this would be the CSP or the CSP's sub-contractor.

Cloud Service Provider (CSP)
The CSP is the organisation responsible for making the cloud service available to enrolled consumers. A CSP acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the cloud consumers through network access.

Data subject
The individual to whom the personal data relates.

Cloud sourcing
The process of outsourcing services, deployment and maintenance to a CSP.

Shrink-wrap terms
Non-negotiable terms in a CSP's standard agreement.

Third countries
Countries outside of the EU/EEA.

Article 29 Working Party (WP29)
Working Party consisting of representatives from the DPA of each EU member state, the European Data Protection Supervisor and the European Commission. The WP29's main objectives are giving expert advice regarding data protection and contributing to a homogeneous interpretation of the EU data protection legislation.

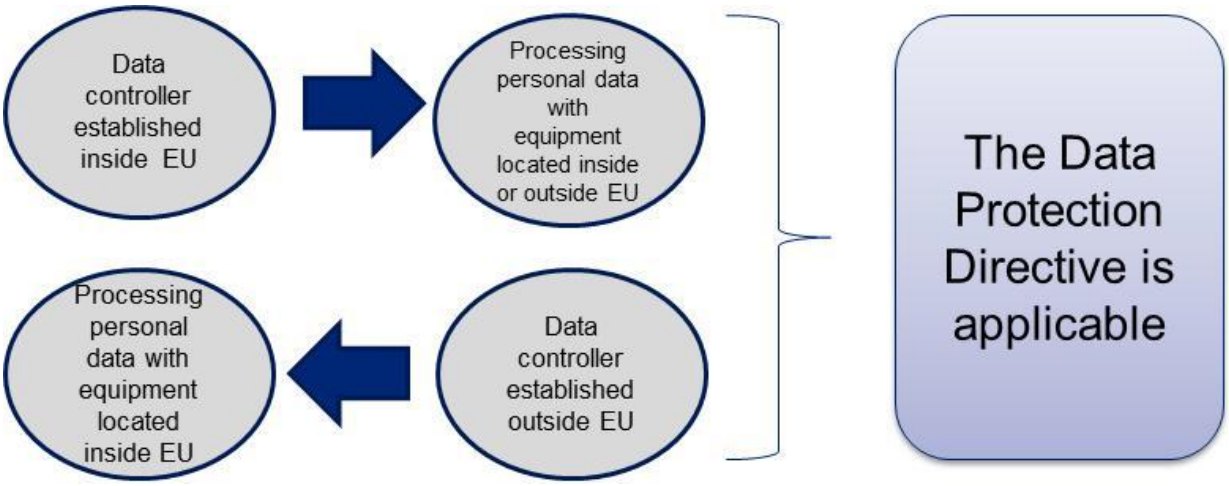
Security measures
Physical, organisational or technical safeguards designed and implemented to protect personal data and safeguard the organisation against information security breaches.

Applicable law

Cloud sourcing is in fact often a multinational outsourcing. For this reason, it is always a good idea to begin the process by establishing which data protection laws are applicable to your organisation, as a data controller.

The focus of this guide is personal data. Subsequently, the one single most important applicable law is the EU Directive 95/46/EC which regulates the processing of personal data, and, of course, the respective national laws in the Nordic countries that implement the Directive.

The requirements following from the Directive are applicable to data controllers established in the EU/EEA as well as controllers established outside the EU/EEA who are processing personal data in the EU/EEA.
The following figure illustrates the situations of data processing where the Data Protection Directive is applicable:



This means that the applicable law depends on the location of the data controller and the location of the data processing rather than the nationality or establishment of the CSP.

In most member states, there are other national legal requirements on the processing of personal information besides the EU legislation. These requirements can differ between the member states. The EU Directive is meant to establish minimum standards that can be implemented more or less restrictively in national legislations. If data is processed in various places with various legal frameworks then the strictest rule will apply.

There might also be national or international legislation on the processing of *non-personal* data which could result in further restrictions in the handling of data in the cloud. One example is international treaties, e.g. the North Atlantic Treaty (NATO), which imposes obligations on all signatories to classify and protect information of common interest. On top of this there could be strictly nationally regulated areas, e.g. on the processing of financial data, data related to research, military intelligence, etc. The guideline will not elaborate further on these regulations.
There might also be legislation in the countries where the data is processed, which affect data controlling organisations directly or indirectly. One example is foreign government's immediate and undisputable access to data, e.g. for crime fighting purposes. The fragmentation and lack of transparency of all laws that might be applicable in specific situations is a risk factor that should not be taken lightly.

Responsibilities

This section identifies the overall areas of responsibilities in a cloud computing partnership, in order to provide a quick overview of the main legal responsibilities that are distributed between the data controller, CSP and subcontractors. How these responsibilities translate into specific tasks and activities will be clarified in the subsequent sections of the guideline.

The data controller is responsible for ensuring that data protection complies with the requirements following from the Directive 95/46/EC. Norway and Iceland are not EU member states but have entered into an agreement with the EU (the EEA Agreement), which means that national legislation must comply with the Directive. Greenland and the Faroe Islands, however, are considered third countries, as they still use an older Danish law from 1978 on public registers, which cannot be considered as corresponding[1]. Public Organisations in Greenland and the Faroe Islands will nonetheless benefit greatly from following the recommendations in this guideline in cloud sourcing situations.

The Directive is implemented via the following national of legislation in the Nordic countries:

Denmark – Persondataloven (429:2000) implementing EU Directive 95/46
(Datatilsynet – www.dt.dk)
Sweden – Personuppgiftslagen (1998:204) implementing EU Directive 95/46
(Datainspektionen – www.datainspektionen.se)
Finland & Åland – Henkilötietolaki (523:1999) implementing EU Directive 95/46
(Tietosuojavaltuutetum Toimisto – www.tietosuoja.fi)
Norway – Personopplysningsloven (31:2000)
(Datatilsynet – www.datatilsynet.no)
Iceland – Lög um persónuvernd og meðferð persónuupplýsinga (77/2000)
(Persónuvernd – www.personuvernd.is)
Greenland – Lov om offentlige myndigheders registre (294:1978)
(Datatilsynet – www.dt.dk)
The Faroe Islands – Lov om offentlige myndigheders registre (294:1978)
(Datatilsynet – www.dt.dk)

Responsibilities as a data controller

First of all it is the data controller's overall responsibility to choose a CSP that guarantees compliance with data protection legislation, since the controller is the main responsible for keeping personal data safe. This carries three immediate responsibilities:

1. Written data processing contract

Organisations are responsible for signing a data processing agreement, stating that the processor solely acts under the instructions of the data controller and that the data processor will implement appropriate technical and organisational measures to ensure the protection of the personal data.

2. If required, obtain approval from the national data protection agency

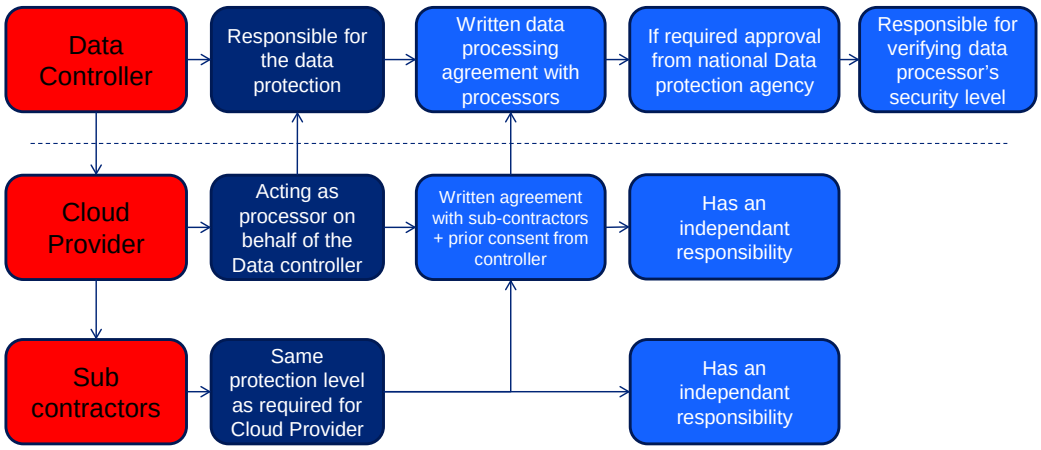
In some Nordic countries, organisations are required to obtain a prior official approval from the national DPA, e.g. if the data processing contains sensitive personal data and the CSP is

[1] http://www.datatilsynet.dk/english/third-countries/

processing data outside the EU/EEA. In some cases approval must be obtained even if the data is non-sensitive. Consult the national DPA's website for further information.

3. Verify the security level of the data processor

It is also the data controller's responsibility to verify whether the CSP lives up to the specific security levels agreed upon in the contract. This verification can be done by assessing documentation provided by the CSP, or under certain circumstances, through onsite control visits by the data controller or an appointed third party auditor.



The figure illustrates the three main responsibilities of the data controller; the written data processing agreement with the processor, approval from the DPA and verifying data processor's security level. Also it illustrates how the CSPs as well as subcontractors have independent responsibilities in regards to written agreements and the overall data protection.

CSP's and subcontractor's responsibilities as data processors

The data processor has an independent responsibility to comply with the data protection legislation defined by the member state in which the processor is established.

Risk analysis

Organisations and administrations wishing to use cloud computing should, as a first step, conduct a comprehensive and thorough risk analysis.

This principle is laid down in the Directive on personal data and is also one of the main conclusions in the article 29 Working Party's opinion 05/2012.

Details regarding the scope and execution of a risk analysis can be found in this guide's appendix 1.

Data processor agreement

The controller of personal data must ensure that there is a personal data processor agreement that meets the requirements of the Personal Data Act in the country where the controller is

situated, as long as the processing takes place within the EU/EEA. Processor agreements are drawn up either through the signing of an agreement with each company that deals with personal data on behalf of the data controller, or by giving a company a written mandate through an agreement to conclude agreements with sub-contractors.

The processor agreement shall:

1. Prescribe that the CSP is obliged to apply to the controllers national legislation regarding processing of personal data
2. Prescribe that the CSP is obliged to take appropriate security measures
3. Prescribe that the CSP may only process personal data in accordance with the instructions of the controller and thereby ensure that the processor does not process personal data for purposes other than those for which the processor has been appointed
4. Ensure that the controller has knowledge of any other processors may come to process the personal data in question
5. Ensure that the controller of personal data has, in an appropriate manner, the possibility to control that the processor meets the requirements of the controller of personal data with regard to the personal data processing and actually takes appropriate security measures

If the data is transferred to third countries, you have five different tools to ensure compliance with the European Commission's standards regarding the security levels outside of EU/ EEA

- Consent
- Secure countries
- Safe Harbor
- Model Clauses
- Ad-hoc contracts

Further elaboration on the different tools as well as details on concrete contractual issues in the data processor agreement can be found in this guide's appendix 2.

Conclusion

The EU Data Protection Directive requires the data controller to conduct a risk analysis in order to establish the appropriate level of security. We advise you to carry out a risk analysis with special attention on cloud specific issues, using ENISAs framework. This should identify all relevant risks and security control measures associated with implementing the cloud service.

As a Data controller you are responsible for signing a written processing agreement, if required obtaining approval from the national DPA when personal data is processed outside of the EU and verifying the security level of the data processor.

If personal data are to be processed by processors in a country outside the EU/EEA, the controller of personal data must ensure that one of the exemptions from the prohibition on

transfer to a third country can be applied, for example consent, standard contractual clauses or adhesion to the Safe Harbor principles.

Finally it is essential to verify the content of the written data processing agreement. Appendix 2 provides you with different choices of contract tools and specific contractual terms which must be included or considered before you sign the final agreement.

Future legislation

With cloud computing being the hot topic that it is and with the great opportunities that follow from these technologies, the EU Commission naturally focuses on the subject of cloud computing in the current formation on data protection regulation.

By the end of 2013, new model contract terms for cloud computing will be published by the EU Commission, and the proposed EU data protection regulation is expected to incorporate new mechanisms that will strengthen the security and clarify the regulation regarding the use of cloud services.

Appendix 1: Risk analysis

Risk Management best practices command that organisations perform a risk analysis before performing major changes that affect the way they manage and control their IT assets. Cloud sourcing can safely be regarded as one such change. And if it involves personal data, then a risk analysis is in most cases strongly recommended or even mandatory pursuant to the Directive on data protection. From the lawmaker's point of view, this requirement will indirectly ensure that "someone" in the data controlling organisation has given a structured thought to the risks that might be involved with outsourcing personal data.

Types of data

The first step in the risk analysis process is to identify the main characteristics of the data and system(s) that the organisation is contemplating to cloud source. The initial mapping will give the manager of the cloud sourcing project a high level overview of possibilities and potential hurdles to the initiative.

The first recommendation would be to clarify the types of datasets to be cloud sourced: What are they about (welfare, tax, infrastructure, health, etc.) and do they include sensitive personal data?

Risk analysis

From the data controller's point of view, conducting a risk analysis serves a number of high ranking purposes:

- Top level management is informed of the cloud sourcing initiative and is forced to consider a course of action
- Weaknesses and vulnerabilities to IT controls are identified
- Appropriate safeguards can be selected.

In the case of cloud sourcing, it is recommended that the risk analysis includes issues specifically related to cloud computing.

The risk analysis should assess the business impact or privacy impact and likelihood of security breaches (loss of confidentiality, integrity and availability). The WP29 also suggests including aspects of transparency, isolation, intervenability, portability and accountability. However, the failure of one of these data protection aspects in a specific cloud service delivery relationship will ultimately result in the loss of confidentiality, integrity or availability.

It is therefore suggested to include specific issues related to cloud sourcing activities in the light of the specific project at hand.

There are different kinds of risk analysis' which can be conducted according to a number of well-known methods. In almost all cases, the organisation will end up with a prioritized list of risks, with each risk comprising an element of business impact or privacy impact and an element of likelihood. For reporting purposes, the risks can be visually mapped in a table like the one below, which is only an example.

Probability	Impact				
	E	D	C	B	A
A	Average	Average	High	Extreme	Extreme
B	Low	Average	High	High	Extreme
C	Low	Average	Average	High	High
D	Low	Low	Average	Average	High
E	Low	Low	Average	Average	Average

Figure 1 - Example of an often used risk mapping model

The business impact of a risk is evaluated on the basis of the expected financial, reputational or administrative consequences of an incident, and it is usually pretty static over time, whereas the likelihood is proportionate with how well or how ill the organisation is protected against the individual risks. It is possible in the same manner to conduct a privacy impact assessment evaluated on the expected consequences regarding e.g. personal information in case of an incident. The likelihood assessment can be based on previous incidents, but it should also always involve a discussion of security measures[2] in place or security measures lacking. Several catalogues of best practice security measures are available. The best known are ISO/IEC 27002, COBIT or NIST SP 800-53. Security measures can be of an organisational, technical or physical nature.

An example of an organisational security measure is the process of *Change Management*. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment can induce undesired risk, especially in the areas of availability and integrity.

Technical security measures include all controls that are implemented, using some kind of technical means, e.g. firewalls or anti-malware scanners on servers and desktop computers. Physical security measures are all the measures destined at physically protecting buildings and equipment, such as locks on doors, firefighting equipment, etc.

In addition, national data protection legislation will often contain mandatory security measures that must be implemented. However, the choice and management of security

[2] Also referred to as *Safeguards* or *IT Controls*.

measures is a specialized discussion, and the organisation should seek the expertise of its information security manager or maybe external consultants if the expertise is lacking in-house. The task is all the more challenging when it involves third party service providers.

A common risk in relation to almost all personal data is the *loss of confidentiality* of the data. In a worst case scenario, loss of confidentiality could e.g. result in a political and public outcry against a minister responsible for the area in question, if social service files from a large number of citizens were leaked. Most organisations would deem such a scenario unacceptable. What are then the security measures available to us to avoid it? It is required to use *strong authentication mechanisms*, e.g. requiring that users provide an additional factor of authentication when they log in (something you have and something to know). The same applies to *encryption of the data*, both at rest and while being transmitted. Of course, once the necessary security measures in the light of the risk analysis have been selected, the next step is to ensure that the CSP is able to offer them as a part of the service. This is where the contract comes into play.

Regarding the specific threats related to cloud computing, ENISA has published a framework[3], which may be helpful in identifying cloud related risks. The Framework is recommended by a number of European DPAs and the WP29.
The framework lists a total of 35 threats with special relevance to cloud sourcing situations. The framework also provides a risk-baseline, listing inherent impacts and probabilities of each threat scenario and a generic bid on whether a given impact and probability is lower, higher or equal in a cloud sourcing situation compared to keeping the service in-house. The organisation should then assess the generic bid against the facts and figures of the contemplated cloud solution. All in all this will give the organisation a well-founded and documented overview of the risk landscape. Again, the process requires certain professional competencies, which the organisation must ensure to bring into play.

One example of a threat in the ENISA framework is *isolation failure*. Isolation failure occurs when mechanisms designed to separate the data and resources of different data controllers in virtual environments fail. The threat is especially relevant because virtual computing is an extremely common component in the providing of cloud services. Both the impact and probability of isolation failure events are set as comparatively *higher* by ENISA from an already high starting point. Vulnerabilities to consider include hypervisor deficiencies and lack of "resource isolation".

For each threat, ENISA's framework also provides lists of vulnerabilities that could promote the occurrence of incidents induced by each threat. As each vulnerability can be controlled by well-known security measures, this part of the threat analysis completes the cataloging of appropriate security measures.

[3] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

Appendix 2: Data processor agreement

This section of the guideline will elaborate on 4 different steps in the assessment and preparation of the contract with the CSP:

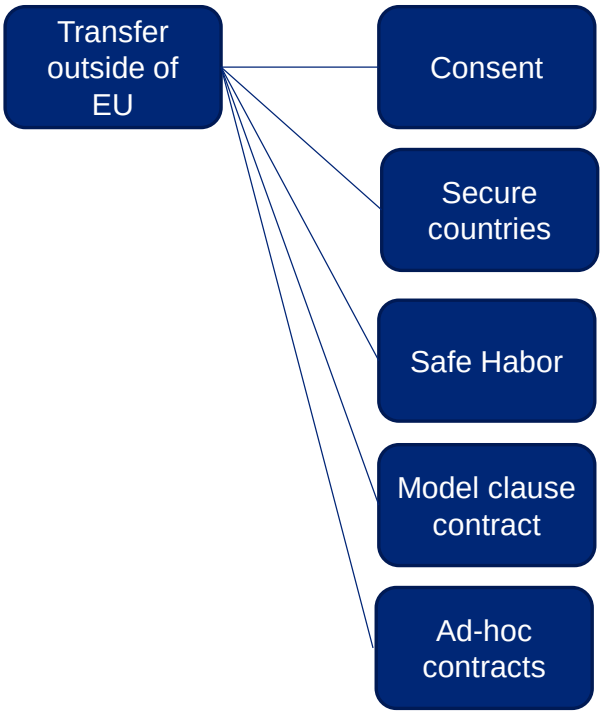
- Issues and solutions regarding data transfers to third countries
- Recommendation of contractual tools to ensure proper form and content
- Specification of the contractual provisions
- Assessment of the CSP security assurance

Data transfers to third countries

Transfer of data for processing in third countries is an entirely distinct discussion when it comes to personal data. The reason for this is, of course, that the legislator wants to limit the possibilities to undermine the EU/EEA protection by transferring data to countries that do not offer the appropriate guaranties. This means that all EU/EEA based data controllers are subject to strict contractual and formal prerequisites, which must be met prior to transferring data outside the EU/EEA. These prerequisites aim at establishing a framework in which adequate levels of protection are obtained from non-EU/EEA processors. To avoid third country challenges, more and more of the larger CSPs offer guaranties that data is only processed inside the EU/EEA.

It is important to remember that once the prerequisites for transfer to third countries have been met all other data protection requirements must *also* be met (i.e. ensuring that data processors take specific security measures or ensuring the contract is adequate in form and content). The general principle is that if the CSP is established outside of the EU, the same European or national legal standards must be complied with, even though the specific third country might not have a corresponding regulation on data protection.

The following scenarios and tools are available to organisations that contemplate to transfer information to third country CSPs.



Consent

Transfer of personal data to a third country is generally possible, if the data controller has obtained the data subject's consent to the transfer prior to the actual data processing. This is by far the most common method to be allowed to transfer personal data to third countries.

Consent from the data subject will allow for the transfer to third countries, but as stated in the previous section, all other data protection requirements must be also be met to comply with data protection regulation.

Secure countries

Transfer to a third country with an adequate protection level (outside the EU/EEA). The European Commission has listed a number of countries, which are considered to have an adequate protection level, either through legislation or through other kinds of precautions. If the CSP is based in one of these countries, the transfer is considered to be as secure as if it was in fact an inter-EU transfer. In other words, the third country aspect does not put supplemental burdens on the organisation.

The third countries with adequate protection levels are[4]:

- Andorra
- Argentina
- Canada (to a certain extent)
- The Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay

Safe Harbor principles

A special tool has been put in place for data transfers to data processors based in the US. These can choose to adhere to 7 "Safe Harbor" principles which are designed to prevent accidental information disclosure or loss. The European Commission has stated that all US companies, which have opted in to the Safe Harbor program are considered to sufficiently protect personal data transferred from Europe.

The Safe Harbor principles can be obtained from the U.S. Department of Commerce[5].

According to the WP29 data controllers should obtain evidence that the Safe Harbor certifications are maintained and request evidence demonstrating that their principles are complied with[6].

Furthermore, in cloud sourcing situations, the WP29 strongly recommends to complement the CSP's Safe Harbor commitment with additional security measures that take the specific nature of the cloud into account[7]. Please refer to the appendix on *risk analysis* for general guidelines on selecting the measures. Remember that the Safe Harbor arrangement does NOT include a standard contract. A real contract in due form must still be concluded between the parties. Approval of the contracts from the national DPA will in some cases be necessary. Please refer to sections below on the *content of the contract*.

The Model clauses:

The European Model Contract Clauses for transferring personal data to unsafe third countries. If public organisations are contemplating to use a CSP that is labeled as "unsafe", the option available is to use the *Model Contract Clauses*. The Clauses can be found on the European Commission's website[8]. They basically make up a contract template (standard contractual

[4] As of 12. December 2012 – Further in: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-4

[5] http://export.gov/safeharbor/eu/eg_main_018475.asp

[6] Section 3.5.1, page 17.

[7] Section 3.5.1, page 18

[8] *http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm#h2-5*

terms) that, if used inter-parties in an unmodified form, is considered to provide an adequate framework for data protection.

In some countries, the usage of the Clauses will exempt data controllers from seeking the competent DPA's approval of the data processing agreement. Organisations should contact their national DPA for specific information.

Ad hoc contracts
If all other options fail, it is still a possibility - although a very rarely used possibility - for the parties to sit down and draft an ad hoc contract. Data transfers based on such contracts can usually only be lawfully carried out after the competent DPA's approval of the contract.
In this case the data controller should contact his national DPA for specific information of approval procedures for these sorts of agreements.

Data processor agreement

Data processing in a cloud must be based on a clear written agreement between the data controller and the CSP (EU Directive's article 17, paragraph 3) and must be concluded regardless of whether any third country data transfer occurs.

Besides the contractual tools aimed at handling third country transfers, which are outlined in the previous section, a couple of other useful contractual tools are available to the data controller.

Model Contract Clauses
As described above, the Model Contract Clauses are originally designed for unsafe third country transfers, as was mentioned earlier on. However, as it is a complete model contract, some Nordic countries recommend, that the Model Contract Clauses can be used as a legal basis for all personal data sub-processing situations, including cloud sourcing and including situations where the CSP is EU/EEA-based (or a Safe Harbor affiliate).

However, it is important to emphasize that the terms included in agreements based on the Model Contract Clauses contract must be complemented with a relevant and thorough set of instructions (purpose limitation) to the processor and with the security measures that result from the risk analysis. Furthermore, the Model Clauses do not reflect specific national requirements that might exist.

Several big CSPs are therefore now offering agreements based on the EU Model Contract Clauses, because this potentially solves the problem of unfitting shrink-wrap terms. However, public organisations that choose to conclude such agreements should be aware of a couple of potential pitfalls:

- In order to be used as intended in arrangements involving third country transfers the Clauses must on most accounts remain unchanged. Several CSPs are known to supplement the Clauses with addendums designed to take precedence over the Clauses, and which aim to "clarify" (in effect, limit) provisions in the Clauses, most notably by adding limitations to the CSP's liability

and the organisation's right to audit. It is therefore advised to submit the full contractual terms to an independent legal review before signing, in order to assess whether it is acceptable in its entirety.

- The Model Contract Clauses only become operational when Appendix 2 to the clauses is filled out. The appendix must contain a description of the technical and organisational security measures implemented by the CSP. These must be in accordance with the controller's instructions to the processor for the processing of personal data.

- The CSP will often be able to supplement the appendix' description with an auditor's statements. The organisation should request to see the full statements, not only the conclusions. This will empower the organisation to make an even more detailed assessment of the adequacy of the CSP's security measures.

Binding Corporate Rules

Binding Corporate Rules (BCRs) were introduced by the WP29 to facilitate groups of companies to make intra-organisational transfers of personal data to unsafe countries i.e. instead of concluding individual contracts between companies that belong to the same corporation the BCRs create a sort of intra-corporate global privacy policy that satisfies EU standards. This guide will not elaborate further on the BCRs, because public organisations are seldom organized like international corporations with internal needs for cross border data transfers.

However, public organisations should be aware that BCRs will also be usable by CSPs in cases where the CSP is made up of several legal entities that all need to enter into play to deliver the cloud service. If this is the case, it should generally be welcomed by organisations, as the CSP's use of BCRs can be seen as a token that the CSP's internal privacy policies have been approved by a competent DPA and that all the CSP's clients are treated equally. However, the CSP will still have to comply with the general legal conditions regarding third country transfers. The WP29 is currently[9] working on setting up an appropriate framework for these types of BCRs.

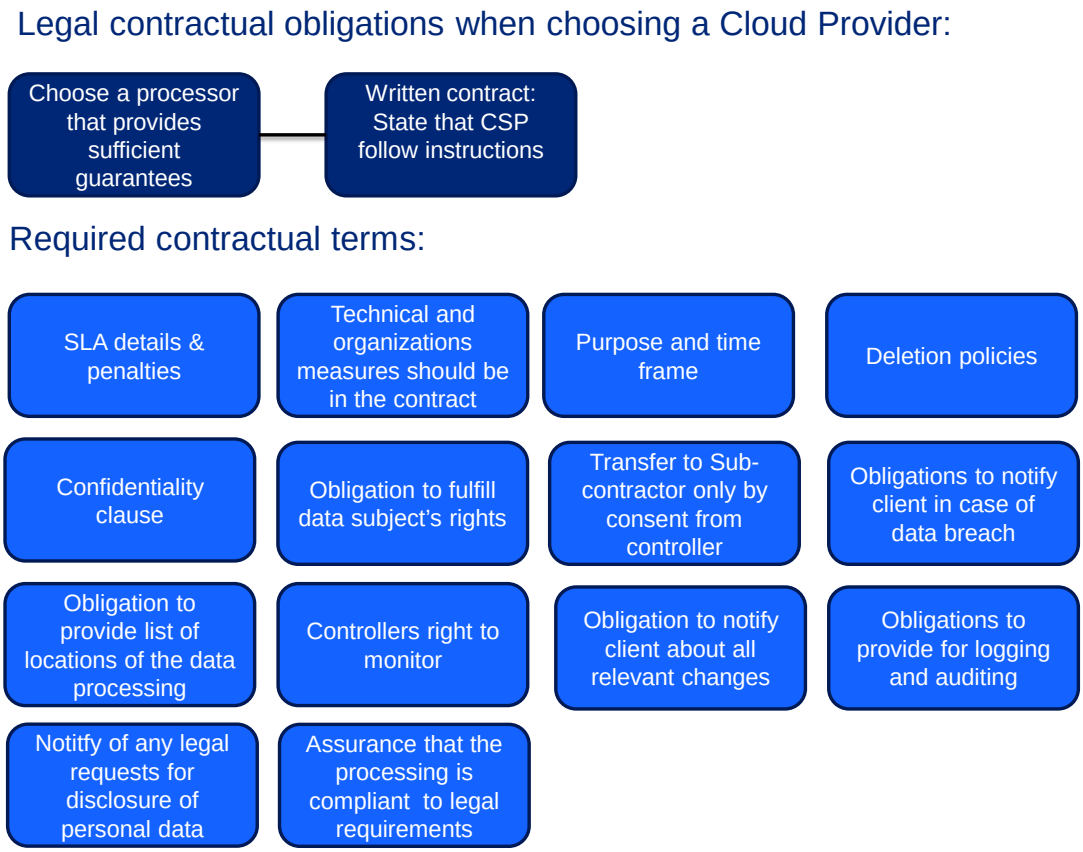
Specify contractual provisions

The contractual tools mentioned above can be helpful to ensure that the right form and content are included in the contract and to improve the degree of control and transparency you will have as data controller.
Aside from the legal obligations in force, the public organisation itself might have its own security standards that need to be considered. Ask your legal department to follow up on the terms proposed by the CSP.

The following is a review of the most important issues that need to be addressed and clarified in regard to a specific service and context, whether you happen to have a Model Clause or a shrink-wrap contract to consider.

[9] As of April 2013

The figure below illustrates first the general contractual obligations that follow directly from the Data Protection Directive and then the mandatory contractual terms that follow indirectly from those two obligations and the current best practice. These terms are the same as those listed by the WP29 opinion.[10]



Each of these contractual terms is addressed below:

Purpose and time frame

Data processing must have a purpose. Data must only be collected for specified, explicit and legitimate purposes, and further processing must not be incompatible with these purposes. A processor agreement should furthermore specify a time frame for both the agreement and the actual processing of data.

Instructions on purpose limitations

The controller must prescribe that the processor may only process personal data in accordance with the instructions of the controller of personal data. The controller shall

[10] [10] Section 4.1, page 21-22.

thereby ensure that the processor does not process personal data for purposes other than those for which the processor has been appointed.

Confidentiality clause
The contract should include a confidentiality clause with regard to personal data that employees at the CSP might come in contact with in the course of delivering the services.

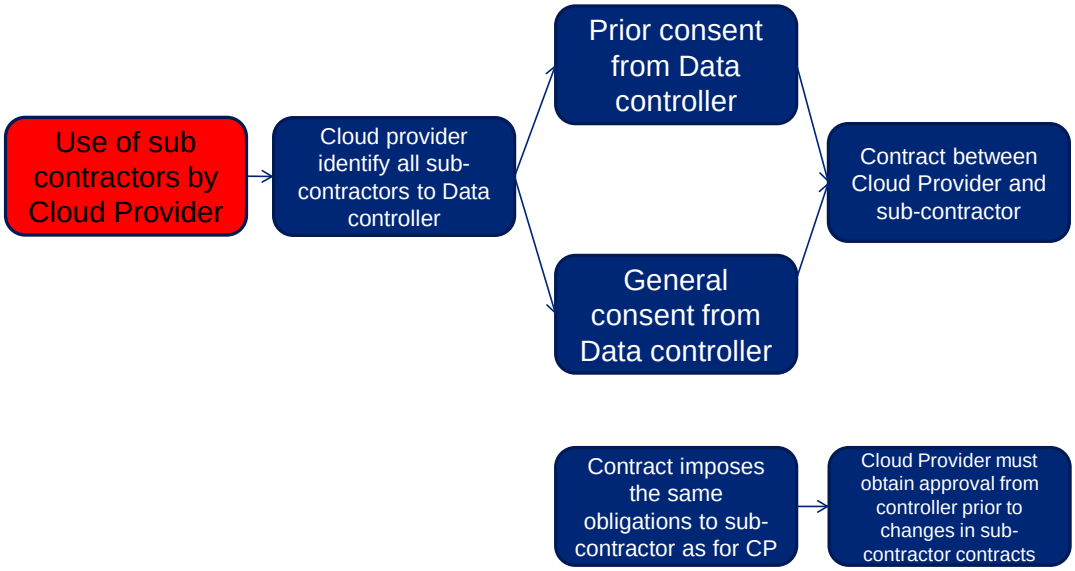
Technical and organisational measures
The technical and organisational measures that the CSP must put in place must be specified. These measures should depend on which kind of personal data is processed. If sensitive data is being processed higher security is demanded.

Deletion Policies
The personal data must be deleted as required and as soon as there is no longer a legal purpose for the data processing – at the time of conclusion of the service or if data subjects ask for it. The contract must therefore include a section on data deletion that covers both live data and data on media bound for destruction.

Data subjects' rights
Data subjects have a number of precise rights with respect to personal data that concerns them (right to information, right to object, access to data, right to rectify). The contract with the CSP must contain appropriate measures to allow the organisation to enforce data subjects' rights against the CSP.

Transfer to subcontractors
Most likely the CSP will engage a number of subcontractors in order to deliver the necessary functionality of the cloud based service. To ensure that this sub-processing does not undermine the actual protection of the personal data, you must ensure that the following terms are in place in your contract:

- Statement of the organisation's consent to the use of subcontractors. This prior consent can be specified as a general approval from the organisation or as separate consents for each subcontractor that the CSP engages with.
- An obligation for the CSP to keep a current list available for the controller of all used subcontractors.
- An obligation for the CSP to ensure that all subcontractors abide by the instructions given by the organisation.
- An obligation for the CSP to ensure that all subcontractors are bound by the same data protection obligations as the CSP itself. The CSP must inform and obtain approval from the data controller prior to any relevant changes in the contract with subcontractor. This includes any changes that can affect the security level.
- Statement that the CSP and/or each subcontractor remain fully liable to the organisation for the performance and potential security breaches of subcontractors.



SLA details and penalties

A Service Level Agreement (SLA) is a part of a service contract where a service is formally defined. The contract should include the instructions to be followed by the data controller in regards to the data processing which is being cloud sourced. The detailed SLA should also be included in objective and measurable terms, and penalties for breach of contract provisions should be specified.

Notifications

The following terms on notification should be in the contract:

- Obligation to inform the organisation in the event of data breaches that affect the organisation's data
- Obligation to inform the organisation in the event of any legally binding request for disclosure of the personal data by authorities in the CSP's country of domicile, unless such notification is otherwise prohibited.

List of locations

The contract should include an obligation for the CSP to provide a list of locations in which the data may be processed. This is an essential part of the transparency obligation of the CSP and has great importance in terms of assessing risks and deciding on the use of contractual tools.

Controller's right to monitor and audit

The contract should include a statement about the controller's rights to monitor and audit - and the CSP's corresponding obligations to cooperate. The right to monitor must be delegable to the organisation's auditor. Please note that several CSPs will try to limit the right to monitor based on the consideration that individual audits of data hosted in a multi-party, virtualized server environment may be impractical technically and can in some instances serve to increase

risks to the customer base as a whole. Instead, the CSPs will often offer to provide a statement by an auditor *chosen by them*. As already stated, organisations should be aware of this discrepancy between their legal obligations and the practical realities of CSP practices.

In this light, some Nordic DPAs have deemed it sufficient if a CSP offers audit statements performed by an independent third party.

Audit Statements

Audit statements come in different forms. They will all tell you something about security measures that are implemented at the CSP, but the scope they cover and the audit activities performed differ from one family of statements to the other. The statements are normally based on control objectives set out by the auditee and the auditor using one of several possible audit and review standards. The statements are usually produced yearly.

This should be kept in mind when organisations assess audit statements against compliance requirements and their own security requirements. The following types of common audit and review standards used in the preparation of audit statements are the most often encountered:

- ISAE 3402 is a global assurance standard for reporting on controls relating to financial reporting.
- ISAE 3000 is used for assurance engagements other than audits or reviews. Typically used for one or more of the following 5 key attributes: Security, availability, processing integrity, confidentiality, privacy.
- ISRS 4400 is used for agreed-upon procedures – agreed between the company and the targetgroup of the statement.
- SSAE 16 is the US counterpart to ISAE 3402. The two can be combined in one statement. SSAE 16 has replaced the well-known SAS70 as of June 2011.

Furthermore, the statements come in two subtypes: In a *Type I* report, the auditor evaluates the efforts of a service organisation at the point in time of the audit to prevent accounting inconsistencies, errors and misrepresentation. The auditor also evaluates the likelihood that those efforts will produce the desired future results. A *Type II* report includes the same information as that contained in a Type I report. In addition, the auditor attempts to determine the effectiveness of agreed-upon controls since their implementation.

In addition to the audit statements, the CSP might also be able to provide a certification in accordance with international information security standards, e.g. ISO 27001. While such certifications are a positive sign that the CSP is working professionally with its security processes, they cannot replace audit statements of the above mentioned type and they cannot solely serve to satisfy the organisation's right to monitor the cloud service.

Notification in case of change

It should be contractually fixed that the CSP must inform the organisation about relevant changes concerning the cloud service, such as the implementation of additional functions. The CSP should ask for approval before implementing larger changes. As data controller you

should specify which changes fall under which category and who carries the risks associated with such changes.

Logging and Auditing

The contract should provide for logging and auditing of relevant processing operations on personal data that are performed by the CSP or the subcontractors. As an example, Danish data protection legislation contains very specific requirements with regard to what information needs to be logged.

Legal compliance

The contract should contain a general obligation on the provider's part to give assurance that its internal organisation and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards.

Contract termination

The contract should contain clear provisions on both the organisation's and the CSP's right to terminate the contract and the conditions that apply in that situation. The provisions should state how and in which form the organisation will receive its data back from the Cloud.