Guidance on the use of cloud

March 2022

DATATILSYNET

Content

1. Introduction

Data protection law is technology neutral and does not specify which kind of software or infrastructure an organisation is required to use for the processing of personal data. This freedom of choice is a strength for each organisation and the organisation is free to choose both the business model and the technology that the organisation itself finds is best suited to the task. At the same time, however, this can be seen as if there is a lack of clear 'yes' or 'no' answers to whether — and if so how — a given solution can legally be used in compliance with data protection law.

One of the technologies which for several years has given rise to questions has been the use of cloud. This is due, among other things, to the fact that cloud services have become widely adopted by the market and that in many areas of business, cloud is the primarily used IT service delivery model.

This guidance is targeted primarily at organisations that would like to start using one or more cloud services(s) and attempts to address the relevant elements of data protection law that you as the controller should consider when you intend to use cloud service(s). However, many of the issues addressed in this guidance apply equally to most other IT service delivery models.

The Danish Data Protection Agency ("the DDPA") also recognises that a large number of cloud services are usually provided as standardised services where each organisation as a customer has limited possibilities to tailor the service in question to the organisation's individual needs and requirements. Parts of the guide are therefore simultaneously *mutatis mutandis* addressed to cloud service providers ("CSP") who can learn more about how they can provide their services in accordance with data protection law.

This guidance contains elements from other guidance published by the DDPA. This includes in particular the DDPA's guidance on transfers of personal data to third countries and the DDPA's guidance on the auditing of data processors, which can both be found on the DDPA's website (in Danish).

Additionally, the European Data Protection Board's ("EDPB's") recommendations for supplementary measures[1] and the guidelines on the interplay between Article 3 and Chapter 5 of the GDPR[2] also provide guidance on issues which frequently need to be assessed when using cloud services.

The use of cloud services does not introduce any new issues in relation to data protection law than other IT service delivery models. However, there are certain elements of data protection law which you must pay special attention to when using cloud services. These include (i) the use of processors and sub-processors, (ii) security of processing, and (iii) transfers of personal data to third countries.

This guidance does not aim to add anything new to the definition of cloud services and does not address the business incentives to use cloud services or lack thereof. Further information on these topics can be found in the Danish Agency for Digitalisation's guidance on the "Use of Cloud Services" (in Danish).

1 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

2 EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

2. What is cloud?

The term “cloud” is generally used to describe a model for providing standardised computer system resources, typically on larger decentralised collections of servers, accessed via the internet.

Cloud can be provided as a service or a collection of services. It may be a simple service which handles specific requests with one or more given parameters – in other words “pure computational power” – or more complex services in the form of complete applications.

Example 1

Scenario 1

An insurance company plans to merge several of its insurance products into one single product. In order to determine an appropriate insurance premium for its new insurance product, the insurance company uses a cloud service to run calculations on a number of datasets derived from its other insurance products that are being merged.

Scenario 2

A chess association publishes a newsletter using a cloud service. On the chess association’s website, members or other interested parties can enter their email address in order to receive the association’s newsletter. Design, publishing and archiving of the newsletters is handled by a cloud service run on a server in the United States and is operated through a web interface.

Scenario 3

A municipality uses a word processor which is run on a server in Ireland and displayed on the users’ screens. The municipality stores all created documents on the municipality’s own server, but the word processing program, including login, setup, hyphenation, spell checking and all other functionality, is done on the server in Ireland.

“Cloud services” is thus a generic term for a wide range of different services. Cloud services can be both highly specialised services tailored to the individual organisation’s needs and fully standardised products used by many customers.

Cloud services can assume many forms and hybrids in both scope of the service and the allocation of tasks and responsibilities between the CSP and the customer. It can therefore often be difficult to get a complete overview of the IT service delivery model used to deliver the services. For instance, the CSP can have a specific task performed by sub-suppliers on the basis of a specific contractual basis with these suppliers. This is the predominant cause of the complex data protection issues associated with the use of cloud services.

A typical characteristic of cloud services is that you as a customer are solely in control over the type of and amount of resources, e.g. storage, processing power, and network topography you require delivered. On the other hand, you are generally not in control over the specific resources provided by the CSP or where those resources are provided. Typically, you can only specify or delimit the location of a resource at a higher level, e.g. for a particular continent or country.

Cloud service models typically describe the content of the resources provided and are often referred to as “xx as a Service”.

Types of cloud services

Infrastructure as a Service (IaaS). IaaS is the most basic of the three service models. With IaaS the customer has access to clean infrastructure which includes basic resources such as processing power, storage, and network. To use the infrastructure, the customer must install and operate all software, both operating systems and applications. Thus, the customer has both control and responsibility for establishing, securing and operating the operating environment, including operating systems, networks, and data storage along with the customer's implemented business applications.

Platform as a Service (PaaS). With PaaS the customer has access to an infrastructure with, among other things, databases, operating systems and core APIs, serviced by the supplier. This infrastructure can be used to implement self-developed or purchased applications. The customer typically has control over and responsibility for the implemented applications and often also the configuration for the application's operating environment. Control over and responsibility for the underlying infrastructure and operating systems is usually left to the CSP. PaaS may also include standardised tools which provide advanced features such as algorithms for big data analysis, artificial intelligence and AI chatbots. The customer will typically use their own applications in interaction with the services included in the platform. As the CSP installs operating systems and services on the infrastructure and also has the responsibility for maintaining them, the customer will typically have no operational responsibility for anything besides the customer's own business applications.

Software as a Service (SaaS). With SaaS the customer has access to the supplier's fully developed, cloud-based business applications. SaaS can be provided by purchasing existing solutions or through a comprehensive procurement of the development and operation of a new solution. Typically, the CSP has full responsibility for the operation and maintenance of the overall solution. The customer has few or no options to customise the solution. This is particularly important if the SaaS solution is to be integrated into an environment of existing systems as adaptations to a SaaS solution may be difficult. In SaaS solutions the CSP is responsible for the operation and maintenance of the solution.

The choice of service model naturally influences the assessments with respect to data protection law that you need to make prior to using the service. The more tasks that are entrusted to the CSP, the more you as the controller must ensure that the CSP performs these tasks in compliance with data protection law including *inter alia* that the CSP ensures the necessary level of security of processing and supplier management. It is you who, prior to the use of a cloud service, must verify and document that the CSP can provide sufficient guarantees that the GDPR will be complied with regards to the processing operations to be carried out by the CSP.[3]

Cloud services can be delivered in several ways with differences in the physical servers and networks from which the services are provided and in the extent to which these resources are shared with other customers. The delivery models are called private, shared, public and hybrid.

Types of cloud delivery models

Private cloud. The cloud service is for exclusive use by and within a single organisation. It may be owned, managed and operated by the organisation itself, a third party

3 See Articles 28(1) and 24 GDPR.

or a combination thereof and may be established within or outside the organisation's own premises.

Shared cloud. The cloud service is for the exclusive use of a well-defined group of organisations. It may be owned, managed and operated by one or more of the organisations in the community, a third party or a combination thereof and may be established within or outside the organisations' own premises. A shared cloud service typically corresponds to the common needs of the participating organisations. At the same time, the governance structures (agreements and governance mechanisms) of a shared cloud service will typically give each organisation a greater influence on governance and development of the service than in a publicly available cloud service.

Public cloud. The cloud service is typically offered on general commercial terms. It may be owned, managed and operated by a company, an academic or a governmental organisation, or a combination thereof. It is established within the CSP's premises and the CSP determines the policies for the service. The publicly available cloud services typically offer the highest capacity, flexibility, and the widest range of services and the fastest development of new services.

Hybrid cloud. The cloud service is a combination of two or more different cloud services (private, shared or public). Each cloud service remains a unique service, but are connected in a way that allows for exchange of data and applications between each service (e.g. for load balancing). A hybrid cloud service is not equal to having multiple individual and uncoordinated cloud services.

The different service and delivery models therefore differ significantly in terms of services, allocation of responsibilities, safety profiles and technical complexity for the customer as well as management requirements. Notwithstanding these differences in service and delivery models, "cloud" is generally characterised by the fact that the resources are not supplied as a product with a lifetime, but as services with a quality criteria which the CSP is responsible for fulfilling.

As the controller you must ensure that all the data protection elements which you consider necessary to impose on and have to possibility to enforce against the CSP are addressed and included in the main agreement and the data protection agreement with the CSP.

Examples of such elements could be:

- Specific predefined security measures *e.g.* measures concerning management of privileged user access and access to personal data;
- The use of sub-processors including in third countries;
- Audits of the CSP and its sub-processors
- Ensuring and documenting that the CSP does not process personal data for other purposes;

Example 2

An insurance company wishes to use a cloud service to handle service and support tickets concerning the company's products. The CSP uses an IT system to document and manage the tickets. The system is run on a server in Germany.

In addition to the processing of personal data in the system on behalf of the insurance company, the CSP offers a 24/7 service desk. To provide this additional service, the CSP has engaged a sub-processor in India. Personal data for which the insurance company is the data controller may therefore in rare cases be accessed by a limited number of employees of the sub-processor in India.

It is the assessment of the insurance company that the personal data cannot lawfully be transferred to the sub-processor in India and therefore opts out of the additional service desk service.

This example illustrates that there may be circumstances relating to the delivery model such as service and support which must also be considered with respect to data protection law. It may be insufficient solely to examine the core service of a cloud service. Any ancillary services where personal data are processed must also be assessed.

A large number of data protection issues arising from the use of cloud are caused by a lack of transparency in how the cloud service is provided in its entirety. Issues may also arise from the fact that contract terms under which cloud services are provided are the CSP's standardised terms of service which cannot be modified to reflect the individual requirements of the controller.

However, processing of personal data by cloud services under a CSP's standard terms of service may well be carried out in compliance with the GDPR. It is, however, your responsibility as the controller to be assured that the processing takes place in compliance with the GDPR and to always be able to demonstrate compliance with the GDPR to the DDPA.

When assessing whether the use of cloud services occurs in compliance with data protection law, the DDPA will attach importance to:

- Your ability to account for your processing activities including data flows;
- Your assessment and documentation of the CSP's ability to ensure that the processing is carried out in compliance with data protection law;
- The wording and transparency of the contract;
- Whether the data processing agreement reflects your requirements with respect to the processing activity for which the CSP is engaged
- Your audits and follow-up of any deviations from the agreement

3. Elements of data protection when using cloud services

As mentioned, data protection law is technology neutral. Therefore, you – as the controller – have full freedom of choice as to which services best meet your business needs.

The DDPA recognises that there may be benefits for organisations in outsourcing their IT infrastructure to a CSP who is specialised in providing infrastructure services. Equally, the DDPA recognises the possibilities of the variety of cloud services which may meet multiple business needs of many organisations. Finally, the DDPA also recognises the developments within the market which mean that many services are provided almost exclusively through the use of a cloud-based IT service delivery model.

However, it should be noted that commercial considerations generally carry little weight in the DDPA's assessment of whether a processing activity is done in compliance with data protection law. Consequently, the setup of an IT system or service cannot justify non-compliance with data protection law.

Below you will find a roadmap to assist you with your assessment of cloud services and CSPs in relation to data protection law.

3.1 Know your services

A basic prerequisite for the lawful processing of personal data is that you are cognisant of and have identified (i) what personal data you are processing, (ii) for what purpose(s) and (iii) how the data are processed.

Based on this mapping, you are able to assess whether the processing activity can take place in compliance with data protection law or if the processing activity, alternatively, should be adjusted accordingly.

You must document these assessments which include in particular the requirements of Chapters II through V of the GDPR and always be able to demonstrate compliance with the law to the DDPA.

The main principle of accountability and the ability to document your compliance[4] is an essential part of data protection law. Your documentation must reflect your considerations and choices — and opt-outs — that you have made with regard to data protection law and is used, among other things, to demonstrate before the DDPA that you – with respect to the specific processing activity – at relevant points in time have assessed the risks to data subjects' rights and have taken the necessary measures to mitigate these risks.

Example 3

A large regional hospital uses a cloud service to process CT scans. The cloud service consists of a computer in Sweden which can produce more image points in the scan than the scanning equipment in Denmark is capable of.

Additionally, the attending Danish physician can – on a case-by-case basis – request suggestions for interpretation of the scans through the cloud service. This is handled by sending the raw data file to a university in the United Kingdom which has developed specialised software for analysing CT scans. The software calculates suggestions for

4 See Articles 24 and 5(2) GDPR.

the interpretation of the image material, and additionally the software uses the raw data file to refine its ability to suggest interpretations.

The service is provided by a Swedish company as a processor for the region, while the British university provides its software as a sub-processor (via the Swedish company) to the region.

It follows from the region's documentation that the scans are uniquely identifiable and are considered personal data. Additionally, the scans contain several metadata such as patient information, location, time and a health history.

Documentation of the processing activity is consolidated from several sources and includes *inter alia*:

a) A complete description of the processing activity including data flows and legal basis for the analysis of the scans and the risks posed by the processing activity to the rights of data subjects.
b) An initial screening of both the Swedish company and the British university to ensure that the organisations' processing will be carried in compliance with data protection law and the data processing agreement(s).
c) A data processing agreement concluded with the Swedish company which reflects the risk assessment pursuant to point (a) and includes *inter alia* the region's instructions for the transfer of personal data to the United Kingdom and applicable transfer tool (the EU Commission's adequacy decision).
d) A guarantee from the Swedish company that its data processing agreement with the British university imposes the same data protections obligations upon the university as the obligations which the Swedish company itself has been imposed by the region. (Alternatively; documentation for the region's review and assessment of the sub-processing agreement between the Swedish company and the British university).
e) A risk assessment concerning security of processing which reflects the fact that the processing activity involves outsourcing and an assessment of the region's implementation of security measures to the risk assessments carried out by the Swedish company and the British University.
f) A description of the established level of security including at the Swedish company and the British university on the basis of the risk assessment pursuant to point (e).

In the opinion of the DDPA, such documentation is generally coherent and consistent with the processing activity carried out.

However, the documentation does *not* include a separate assessment of the legal basis on which personal data may be disclosed to the university for its own purposes, in particular the improvement of the software's ability to suggest interpretations.

This example illustrates the many aspects of a processing activity which need to be identified, assessed, and documented, prior to using a cloud service.

Also note that the processing of personal data entrusted to the data processor by the data controller for the processor's own purposes is considered as a disclosure of personal data between two controllers. As such, a legal basis for the disclosure must be identified and the original controller must additionally assess whether the disclosure is incompatible with the original purpose(s) of the processing.

3.1.1 Risk assessment concerning data protection

Knowing your processing activity is the basic prerequisite for assessing the risks to the rights and freedoms of the data subject posed by the processing and implementing technical and

organisational measures to ensure that these risks are mitigated and that the processing activity is lawful.

In other words, you have to carry out a risk assessment concerning data protection pursuant to the provisions on the responsibility of the controller and on data protection by design and by default.[5] This risk assessment should not be confused with the risk assessment concerning security of processing which is discussed in detail in section 3.1.2 below.

For instance, when processing personal data using an IT system there may be a risk of collecting more personal data than necessary for the pursued purpose or a risk that the data subject will not receive the information required pursuant to the controller's notification obligation. The provision on data protection by design and by default require you to implement technical and organisational measures to mitigate such risks.

Your risk assessment concerning data protection must be carried out on the basis of the intended processing activity as a whole. If the processing activity is supported by an IT system, the system and its layout shall also be included in the assessment.

However, as mentioned above, cloud services are characterised by the fact that they are provided as standardised solutions where there is no or only limited possibilities for you as the controller to tailor to the service delivery model or applications to your requirements. Therefore, there may be limited possibilities to implement the necessary technical measures required to address any potential data protection risks or – alternatively – to modify the system in such a way that the identified risk is completely eliminated.

This means that there may be – based on your risk assessment concerning data protection – cloud services which you will need to opt out of if there no possibility to implement the technical measures that you consider necessary.

This will most often be the case for SaaS-solutions as the control over the solution in these cases mostly lies with the CSP. It may, however, also be the case for PaaS and IaaS solutions.

Before initiating or substantially altering a processing activity, you must carry out a risk assessment concerning data protection. Based on this risk assessment, you can assess whether the intended cloud service can support your processing activity without leading to higher risks for data subjects.

With respect to using cloud services, it is particularly relevant to assess *inter alia* the following, if possible, in cooperation with the CSP where appropriate:

- Does the CSP process any additional personal data than the personal data entrusted to the CSP by you? This may *e.g.* include collection of metadata or other service data. If this is the case, you will need to assess who is the controller for the processing of this personal data etc.
- Does the CSP process the personal data entrusted to the CSP for its own purposes? If this is the case, you will need to assess whether the personal data can be disclosed to the CSP and on which legal basis.

3.1.2 Risk assessment concerning security of processing

For any processing activity you must – most often together with your data processor (in this case the CSP) – establish an appropriate level of security of processing.

5 See Articles 24 and 25 GDPR. A detailed examination of this can be found in the DDPA's guidance on security of processing and data protection by design and default (in Danish).

As a prerequisite for establishing and maintaining an appropriate level of security of processing, you must assess the risks to the rights and freedoms of data subjects. In other words, you must carry out a risk assessment.

The DDPA recognises that this may be a difficult task for the individual controller. Nevertheless, an overview of the threats to the data subjects' rights and freedoms which you need to protect against is a basic prerequisite for establishing an appropriate level of security.

Like any other use of processors the use of CSPs has the implication that it is no longer you as the controller but rather the CSP who is tasked with implementing the required security measures in practise. Additionally, it is customary for CSPs to have established a certain level of security of processing already when the CSP starts providing one or more services in the market. Your task as the data controller is therefore, with the assistance of the CSP, where appropriate, to:

- Identify which level of security of processing the CSP has established including by reviewing the CSP's documentation and, where appropriate, through an in-depth dialogue with the CSP;
- Review whether this level of security of processing corresponds to the level that you as the controller – on the basis of your own risk assessment – consider appropriate;

The DDPA recognises that many CSPs will have appropriate – or even beyond appropriate – level of security of processing for the majority of processing activities entrusted to the CSP by its customers. Your task as the controller is therefore often "just" to verify that this is the case and to document your assessment.

However, there may be cases where you have a special processing activity which includes *e.g.* the processing of health data to on a large scale where you consider that additional measures beyond those already implemented by the CSP are necessary. In this case, you must ensure that you are entitled under the contract(s) with the CSP to request the CSP to implement these additional security measures that you consider necessary.

Additionally, you should also pay attention to the allocation of tasks and responsibilities between you and the CSP with regards to your processing activity. If the processing activity has previously been carried out by you alone, engaging a CSP is likely to require you to revisit your risk assessment and existing security measures as the use of a data processor is likely to alter the risk landscape for your processing activity. Consequently, it is likely that you must review your existing security measures as a result of the changed allocation of tasks and responsibilities between you and the CSP including *e.g.* controls concerning privileged access management, change control etc.

Example 4

A municipality uses an IaaS solution where personal data are transported/routed in transit through a third country. At no point will the personal data be processed in the third country beyond the transmission itself.

In principle, this does not constitute a third country transfer within the meaning of Chapter V of the GDPR.[6]

However, the municipality must still ensure an appropriate level of security of processing *inter alia* to prevent access to personal data by public authorities for surveillance purposes directly through the cable transmission. In practice, this will often be done by assessing to which extent the security measures implemented by the IaaS-supplier are adequate.

6 EDPB's guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

For instance, if the IaaS-supplier has only implemented transport encryption using keys that are managed by the IaaS-supplier, it may be a necessary additional security measure for the municipality to ensure that the content itself is encrypted during transport using keys that are managed by the municipality in the EU/EEA.

3.2 Know your supplier

When using cloud services the CSP will usually process personal data on your behalf as a processor. As such, the CSP may only process personal data on your instructions.

For this reason you are required to conclude a data processing agreement with the CSP. The agreement must meet a number of minimum requirements and must include *inter alia* your instructions to the CSP and the agreement must, in general, establish the framework for the CSP's processing of personal data on your behalf. For more details on the conclusion of data processing agreements see section 3.2.2 below.

3.2.1 Screening of supplier(s)

Generally you have full freedom of choice with regard to which CSP you wish to engage for the processing of personal data.

This freedom of choice is limited only by the fact that you may only use a CSP who can provide sufficient guarantees that the CSP will comply with data protection law when processing personal data on your behalf.[7]

This entails that you must perform a screening of the potential CSP(s) in advance to assess whether the CSP will be able to meet the data protection requirements that you consider appropriate for your processing activity.

In the opinion of the DDPA, this screening can advantageously be based on the data processing agreement that you intend to enter into with the CSP. This may include *inter alia* the DDPA's standard data protection clauses, the EU Commission's data protection clauses[8] or the CSP's own data processing agreement.

For the purposes of your screening you should have the following questions answered by the CSP; either through a dialogue with the CSP or by reviewing the CSP's documentation:

a) Is the CSP – pursuant to the data processing agreement – under an obligation to process personal data only on your documented instructions or does the CSP reserve the right to process personal data for its own purposes?
b) Does the CSP have policies and procedures in place to ensure that its employees have committed themselves to confidentiality or are subject to other appropriate obligations of confidentiality, and can the CSP demonstrate compliance with these?
c) Has the CSP – taking into account the allocation of responsibilities between you and the CSP – established an appropriate level of security of processing with respect to processing activity with which the CSP has been entrusted?
d) Does the CSP have a procedure for screening any sub-processors in order to ensure that the sub-processors will also be able to comply with the data protection requirements imposed on the CSP by you and, if in the affirmative, does the procedure include dissemination of the sub-processors' documentation to you?
e) Does the procedure referenced above include a deadline for the CSP's submission of documentation of the CSP's screening of sub-processors and is the deadline in

7 See Article 28(1) GDPR.

8 On 4 June 2021, pursuant to Article 28(7) GDPR, the EU Commission published a set of standard contractual clauses which are similar in nature to the DDPA's standard data protection clauses. Learn more here: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/okt/databehandleraftale-skal-jeg-bruge-dansk-skabelon-eller-eu-standardkontraktbestemmelser (in Danish)

line with the deadline for notifying you of the use of new sub-processors or of changes to the current sub-processors?

f) Does the sub-processor agreement (if any) reflect the same requirements that will be imposed upon the CSP by you as the data controller?
g) Does the CSP have a complete overview of the sub-processors that the CSP has engaged for the provision of its services including in which countries, especially outside the EU/EEA, these sub-processors are located, and from which countries the CSP and any sub-processors can access the personal data? If so, has the CSP established a transfer tool that is effective in view of the processing activity you have entrusted to the CSP?
h) Having regard to the entrusted processing activity, does the CSP have procedures in place to assist you in handling requests from data subjects under Chapter III of the GDPR?
i) Does the CSP have procedures in place for handling personal data breaches and do these procedures include the CSP's assistance to you with your obligation to notify personal data breaches to the DDPA?
j) Can the CSP delete or return the personal data at the end of the processing operation?[9]
k) Does the CSP have a procedure in place to assist you in your audits of the CSP or for carrying out audits by independent third parties such as auditors?

For some of the abovementioned items, there are a number of specific factors you must pay special attention to when reviewing the CSP's documentation or in your dialogue with the CSP.

In particular on point (a)

The CSP may (with regard to the processed personal data) only act in accordance with the instructions given by you as the controller. Therefore, the CSP may not, as a general rule, process the personal data entrusted to the CSP for the CSP's own purposes, unless required to do so by EU or Member State law to which the CSP is subject.

If a CSP processes personal data for the CSP's own purposes without authorisation from you as the controller, it will (i) constitute a personal data breach for the controller and (ii) the CSP will be considered to be a controller in respect of that processing activity.

In the opinion of the DDPA, a CSP's processing of personal data for the provider's own purpose(s) shall be regarded as a disclosure of personal data to the CSP which requires a legal basis.

If you wish to authorise the CSP to process personal data for the provider's own purpose(s) or wish to engage a CSP who reserves the right to process personal data entrusted to the provider for its own purposes, note the following:

a) The purposes for which the CSP wants to process the personal data must not be incompatible with the purpose(s) for which you have originally collected the personal data;
b) You must identify a legal basis for disclosing the personal data to the CSP for the purposes of the provider's own processing activities. Additionally, the CSP must also identify a legal basis for its processing;

Further, the DDPA notes that in cases where the CSP generally reserves the right to process personal data entrusted to the CSP for its own purposes, all personal data entrusted to the CSP shall be considered disclosed to the CSP – and not only the personal data which the CSP actually decides to process for its own purposes. This is because, in the case of such a general reservation, the CSP, in fact, has control over all the personal data entrusted to it and deter-

9 There may inter alia be circumstances related to the use of shared hardware by the CSP which entail that the supplier is unable to ensure the effective deletion of the data, and the CSP may be subject to third country law under which the supplier is not entitled to erase the data. It should be noted that compliance with the legislation of third countries cannot justify a derogation from the obligation to delete.

mines which personal data the CSP wishes to process. Therefore, the CSP must be considered as the controller for all the data including the personal data which the CSP decides not to process for the provider's own purpose(s).

In addition, as the controller you must – in the view of the DDPA – ensure[10] to a certain extent that the recipient to whom personal data is disclosed has a legal basis for the processing of this personal data.

If you are aware or become aware that it is unlikely that the CSP will have a legal basis for the provider's processing of the personal data for its own purposes, it will not be lawful for you to disclose the data to the CSP.

Therefore, you should carefully review the data processing agreement that you intend to enter into with the CSP to determine whether – and if so to what extent – the CSP intends to process the personal data entrusted to the CSP for its own purposes.

Example 5

A consultancy firm wants to migrate to a cloud-based customer relationship management system (CRM system) and intends to process information concerning name, professional email addresses, and information concerning performed work and customer feedback in the system.

A detailed examination of the terms of the contract including the data processing agreement under which the CSP offers the CRM system shows that the CSP pseudonymises the personal data recorded in the system and processes the pseudonymised information for the purposes of (i) improving the functionality of the system and (ii) internal reporting and modelling *e.g.* capacity planning etc.

The consultancy company considers that the processing of personal data by the CSP for its two above-mentioned purposes is not incompatible with the purpose(s) for which the consulting company initially collected the data and that the CSP's processing of personal data for the two purposes is carried out for the purpose of legitimate interests pursued by the CSP.

In this case, the processing of personal data by the CSP for its own purposes is not an obstacle for the consultancy firm's use of the CSP. Note, however, that the CSP is independently responsible for the processing of personal data for the above-mentioned two purposes in compliance with data protection law.

In particular on point (d)

As mentioned above, pursuant to the GDPR you may only engage a processor who can provide sufficient guarantees that the processor will comply with data protection law when processing personal data. This obligation is not limited to the primary data processor that you engage. In addition to the CSP itself, you must ensure that any use of sub-processors by the CSP will also be done in such a way that the processing complies with data protection law.

In essence, the rights and freedoms of the data subject must enjoy a consistent level of protection throughout the supply chain and the level of protection must not be lowered by the fact that the processing activity is entrusted to a sub-processor.

In practice, it is natural that the CSP screens any sub-processors engaged by the CSP to ensure that the sub-processors can also comply with data protection law. However, the results of these screenings must be available to you as the controller as part of the CSP's documentation or be provided to you upon request in order for you to verify these screenings.

10 Pursuant to the principle of lawfulness in Article 5(1)(a) GDPR.

You should also be aware of this requirement when the CSP replaces any sub-processors. Therefore, the CSP's procedures for the screening of sub-processors should also include the submission of sub-processors' documentation to you together with the CSP's potential requests for a specific authorisation for the use of a new or another sub-processor or when the CSP notifies you of the intended use of a new or another processor (in cases where the CSP has a general authorisation).

In particular on point (f)

It is also a requirement under the GDPR that the CSP imposes the same obligations on its sub-processors, if any, as are imposed on the CSP itself under the data processing agreement concluded between the CSP and you as the controller.

This is usually done through the conclusion of sub-processing agreements between the CSP and any sub-processors.

It is not required that the sub-processing agreement is identical in wording to the data processing agreement that you intend to enter into with the CSP. On the contrary, the sub-processing agreement must be seen in light of the specific processing activities entrusted to the sub-processor. However, the sub-processor must in essence be subject to the same data protection obligations as the CSP will be subject to.

By way of example, if the CSP, pursuant to its data processing agreement, is under an obligation to request your prior specific authorisation for or (in the case of a general authorisation) to notify of the replacement of a sub-processor with 6 months' notice, it is insufficient if the sub-processor, pursuant to the agreement between the CSP and the sub-processor, is required to notify the CSP only with 30 days' notice.

In particular on point (g)

A CSP commonly relies on a number of sub-processors for the provision of its service(s).

As the controller you need to have a complete overview of which processors – beyond the CSP itself – you engage for the processing of personal data. You need to map all the sub-processors engaged by the CSP and any further sub-processors that may be found in the supply chain.

This is because you, as the controller, must be able to demonstrate that all processors – the CSP and any sub-processors – can provide sufficient guarantees that the processing of personal data will take place in compliance with data protection law.

This is also due to the fact that personal data may only be transferred to countries outside the EU/EEA on documented instructions from you as the controller. You must therefore actively consider whether you wish to instruct the CSP to transfer personal data to any sub-processors used by the CSP and located in third countries. See section 3.4 below for further details.

3.2.2 Conclusion of a data processing agreement

When using a CSP you are normally the controller with respect to the personal data while the CSP is a processor. Accordingly, a data processing agreement must be concluded between you and the CSP.

Pursuant to the GPDR, a valid a data processing agreement must meet a number of minimum requirements. In particular, the data processing agreement must be in writing, including in electronic form.

A data processing agreement shall *inter alia* set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the data controller and the data processor's duties in relation to the processing activity.

For further details on data processing agreements and the minimum requirements, please refer to the DDPA's guidance on controllers and processors, the DDPA's standard data processor agreement approved by the European Data Protection Board (in Danish) and the EU Commission's standard clauses pursuant to Article 28(7).

3.3 Auditing the CSP and sub-processors

As the data controller, you have an obligation to audit your processors to ensure that they – like yourself – process the personal data in compliance with data protection law. This also applies when you entrust the processing to one or more CSPs.

The DDPA has issued general guidance on auditing data processors (in Danish), where you can learn more about how and how often you should audit your processors. Below you will find a brief description of the factors that you should take into account in your assessment of how and how frequently you must audit your processor(s).

3.3.1 Intensity

Generally, the more that may go wrong with respect to the processing activity performed by the processor (higher risk), the higher are the requirements for your audits of the processor. When it comes to data protection, you should be aware that this assessment is not based on your (as a company or as a public authority) possible incompliance with the law. Rather, your assessment must be based on the risks to the data subjects such as employees, customers, and citizens; what is the likelihood of something going wrong, and what the consequences are if the scenario actually occurs.

As a rule of thumb, you can assume that the requirements for your audits of data processors increase as:

- the processor processes **more** personal data;
- data becomes more **confidential** or **sensitive**;
- the processing becomes more **intrusive**;

3.3.2 Frequency

The more critical the processing is for the data subjects, the more intensive checks of the data processor you will have to carry out. Consequently, it may in some cases be necessary to audit the processor's compliance with its obligations annually. Similarly, it may – depending on the circumstances – be sufficient to audit the processor at a lower frequency if the risks to the data subjects are low.

Factors which indicate a higher or lower frequency

Examples of factors that may indicate the necessity of a higher frequency of audits:

- The processor has in the past had difficulties complying with agreements (not just the data processing agreement).
- The processor has experienced several serious security breaches, including personal data breaches. Naturally, this presupposes that you are aware of such breaches. However, in some cases you will become aware of breaches, for instance when a breach causes interruptions to your service and you request an explanation for the interruption in your service, whereby the processor cannot hide the cause or severity of the breach. With respect to personal data breaches, it is a legal requirement that the processor notifies you of such breaches without undue delay.
- Sub-processor(s) are often replaced.
- There are often acquisitions, changes of ownership, mergers, or significant changes in the business strategy of the processor. You will often notice such things as a customer. Change of ownership/mergers can at first appear insignificant, especially if the data processing agreement is still in force, but they may significantly alter a company's strategy and, consequently, the company's priorities with respect to security of processing. Change of ownership may also in the transition period lead to a loss of focus on the protection of certain parts of the IT environment both in relation to the administration of the

environment and the physical movement, replacement, or discarding, of equipment.

Examples of factors that may indicate a need for audits outside the ordinary frequency:

- Change of ownership, mergers, or radical changes in the strategy of the processor.
- A pandemic changes the way in which work is carried out including the access to personal data (more work from home and significant changes in the prerequisites for the use of the service).

Examples of factors that may indicate a need for a lower frequency of audits:

- Long experience with the processors (data processor and sub-processors) which shows a stable service and no or few serious security breaches.

3.3.3 Specifically for cloud service providers

The DDPA recognises that CSPs usually – as part of their general information security management systems – have established procedures for carrying out audits and have audits carried out by one or more independent third parties who draw up audit reports.

In this context, it will normally be sufficient for you to review the audit reports annually prepared by the independent third parties engaged by the CSP.

However, it is important to be aware of the audit reports' scope and whether the reports cover the processing activities that you have entrusted to the CSP.

If this is not the case for the audit reports drawn up on the CSP's own initiative, you must ensure that you, pursuant to your agreements with the CSP, are entitled to require an audit under a different scope and using other methods which will cover your processing activities.

3.4 Transfers to third countries

If you intend to use a CSP that is located in a country outside the EU/EEA – a so-called third country – or uses one or more sub-processors located outside the EU/EEA, you must pay special attention to a set of specific requirements. In this context, in July 2021, the DDPA revised its guidance on transfers of personal data to third countries (in Danish) which elaborates on those requirements in further detail.

When you intend to entrust one or more processing activities to a CSP you can with regards to compliance with the specific requirements – the rules in Chapter V of the GDPR – advantageously rely on the roadmap set out in the EDPB's recommendations on supplementary measures[11].

This means that you have to:

1) Identify your third country transfers
2) Identify or establish the relevant transfer tool that you are relying on;
3) Assess whether the Article 46 transfer tool you are relying on is effective in the light of all the circumstances of the transfer and, if not,
4) Adopt supplementary measures;
5) Observe any procedural requirements; and
6) Re-evaluate transfers at appropriate intervals;

11 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

In particular on point (1)

When you need to identify whether personal data will be transferred to third countries in connection with your use of a CSP and, if so, which countries specifically, you can advantageously rely on the mapping of where personal data is processed that you have carried out in the context of your screening of that provider. See section 3.2.1 for further details on this mapping.

Your mapping shall *inter alia* discern whether personal data are processed by one or more processors in third countries and whether personal data are or will be accessed by processors in third countries. In the affirmative, you must enter into a data processing agreement instructing the CSP to transfer the personal data to these processors in the concerned third countries and establish a valid transfer tool.

All transfers of personal data require a transfer tool. This applies to everything from the processing of personal data in connection with service and support functions to the transfer of personal data for the purposes of troubleshooting the CSP's infrastructure.

It is not uncommon for CSPs' documentation to include only a general list of all sub-processors engaged by a CSP for the provision of its services. Therefore, if you only use some of the cloud services offered by the CSP, not all listed sub-processors are necessarily relevant for your processing activity. You can advantageously engage in dialogue with the CSP about which specific sub-processors are relevant for the services that the CSP provides to you.

However, it is your responsibility as the controller to be able to document this before the DDPA. If you are unable to engage in dialogue with the CSP or if your dialogue with the CSP does not provide you with sufficient information to be able to document before the DDPA which specific sub-processors are relevant for the services used by you, you must, in the view of the DDPA, assume that all the sub-processors listed in the CSP's general list are engaged for the provision of your cloud services.

In particular on point (2)

If the CSP or its processor(s) is/are located in one of the countries where the European Commission has found that the third country ensures an adequate level of protection, you may sufficiently refer to the adequacy decision of the European Commission as your transfer tool.

If the CSP or its processor(s) is/are not located in such a third country, you will most often establish the required transfer tool by entering into standard contractual clauses adopted by the European Commission with the CSP etc.

Where the CSP has engaged one or more sub-processors in third countries, the CSP will most often already have entered into standard contractual clauses with that sub-processor, thereby establishing the required transfer tool.

However, it remains for you as the controller to ensure – and to be able to document before the DDPA – that a valid transfer tool to the third country in question has been established.[12]

Standard contractual clauses

One of the most relied upon transfer tools are the European Commission's standard data protection clauses – also known as SCCs – which exist as a template to be completed and signed by the data exporter and the data importer. Both the European Commission and the supervisory authorities have the possibility to adopt standard contractual clauses, but so far only the European Commission has taken advantage of this option.

[12] See Article 44 GDPR which contains the general principle of transfer of personal data to third countries. It follows from that provision that a transfer may take place only if, subject to the other provisions of the GDPR, the conditions set out in [Chapter V] are fulfilled by the controller and the processor. (The DDPA's emphasis).

On 4 June 2021, the Commission adopted new SCCs for data transfers to third countries which consist of several modules to be selected appropriate to the situation. Since 27 June 2021 it has been possible to conclude SCCs in the following four situations:

- Module 1: Transfers from controller to controller
- Module 2: Transfers from controller to processor
- Module 3: Transfers from processor to processor
- Module 4: Transfers from processor to controller

You may conclude SCCs and rely on them as your transfer tool without prior approval from the DDPA. However, you should always ensure that you as a data exporter have applied the SCCs correctly and that you and the data importer are able to comply with the obligations arising from the SCCs.

The new SCCs contain a so-called "docking clause" that allows for the continuous replacement or addition of parties to the agreement which may be particularly relevant for more complex processing activities.

Additionally, you may include the SCCs as part of a broader contract between you and the data importer and add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the SCCs. For example, you may include clauses on the application of supplementary measures without requiring approval from the DDPA.

Any alteration of the wording of the SCCs will entail that the SCCs become a so-called ad hoc clauses whose use requires prior approval from the DDPA.

In particular on points (3) and (4)

In July 2020, the Court of Justice of the European Union ("the CJEU") ruled in the so-called Schrems II-judgment that a transfer based on appropriate safeguards such as the Commission's SCCs must afford the data subjects a level of protection of their personal data essentially equivalent to that guaranteed within the EU/EEA.

This means that you must assess if there are laws and/or practices in the relevant third country or countries which may impinge on the effectiveness of the concluded SCCs. For instance, this may be the case if there are laws and/or practices in the third country which allow for the collection of or access to the transferred personal data by law enforcement authorities in a way that does not meet European standards.

If this is the case, you have three options according to the EDPB's recommendations.

You may **(i)** refrain from initiating the transfer or suspend the transfer, if ongoing, which in practice is likely to entail not using the cloud service in question.

Alternatively, you may **(ii)** implement supplementary measures to ensure an essentially equivalent level of protection to that guaranteed in the EU/EEA. To this effect, the EDPB has published a set of recommendations detailing how to assess the level of data protection in a third country and what supplementary measures you may implement if necessary.

If supplementary measures are necessary, you are likely required to implement technical measures whereas contractual and organisational measures will often not be sufficient to address the "problematic" legislation and/or practice.[13] However, this requirement is based on the specific circumstances of the "problematic" legislation and/or practice. According to the EDPB, combining diverse measures in a way that they support and build on each other may

13 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 53.

enhance the level of protection and may therefore contribute to reaching EU standards.[14] However, the DDPA notes that in cases where "problematic" legislation and/or practice allows for access to personal data by public authorities in third countries, in particular for surveillance purposes, in a manner not compliant with EU standards, typically only supplementary technical measures may impede or render such access ineffective.

It is not decisive whether you as the controller or the CSP implement the supplementary measures provided that the measures are effective. However, there are types of supplementary measures, in particular implementation of effective encryption, which may be difficult for the CSP to implement. This is, in particular, the case where the CSP itself will be in possession of the encryption keys for which reason the encryption cannot be considered effective. In any case, where the CSP can, in fact, implement supplementary measures, it remains your responsibility as the controller to ensure that the supplementary measures implemented by the CSP are effective and, in combination with the relevant transfer tool, ensure an essentially equivalent level of data protection to that in the EU/EEA.

Additionally, the DDPA recognises that assessing legislation and practices in a wide range of third countries where a CSP and its (potential) sub-processors are located can be quite extensive. In this respect, it is the opinion of the DDPA that you may take a "worst case scenario" as the basis of your assessment *i.e.* base your assessment on the assumption that all the concerned third countries have "problematic" legislation and/or practice and, on this basis, assess in more detail which supplementary technical measures must be implemented to ensure an essentially equivalent level of protection to that in the EU/EEA.

Finally, you may **(iii)** decide to continue the transfer without being required to implement any supplementary measures, if you consider that you have no reason to believe that the relevant and "problematic" legislation will be applied, in practice, to your transferred data and/or CSP including any sub-processors.

In this case, you must demonstrate and document in your assessment, where appropriate in cooperation with the CSP, that the legislation and/or practices are not interpreted or applied to the transferred data and/or the CSP.[15] However, it is insufficient as documentation to refer to your own – or the CSP's – subjective assessment that the transferred personal data is not of interest, for instance to law enforcement authorities, if this statement is not supported by objective, trustworthy and accessible information *e.g.* from the concerned authorities.

Paragraphs **(ii)** and **(iii)** mentioned above are examined in section 3.5 below with respect to the United States.

3.5 Cloud and the United States

In relation to the GDPR, the United States is considered a third country and Chapter V of the GDPR must be complied with when transferring personal data to the US.

Since the CJEU's judgment on 16 July 2020 in the so-called Schrems II case, there is no longer a valid adequacy decision by the European Commission which finds that the US provides an adequate level of protection. Therefore, in order to transfer personal data to the US in connection with the use of cloud services, you must establish appropriate safeguards *e.g.* enter into the SCCs with the CSP.

For a general overview of the Schrems II-judgment and the impact of the judgment on the transfers of personal data to the United States, see the DDPA's news of the Schrems II-judgment (in Danish), the EDPB's recommendations 02/2020 on the 4 essential guarantees and recommendations 01/2020 on supplementary measures.

14 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 52.

15 See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraphs 43.3, 45-47, and Annex 3, for further details on the requirements for this assessment.

In summary, in the case of the US, the CJEU considered that neither Section 702 of the Foreign Intelligence Surveillance Act (FISA) nor Section E.O. 12 333, read in conjunction with the Presidential Policy Directive-28 (PPD-28), meet the proportionality requirements of EU law, with the result that surveillance programmes based on these provisions cannot be considered to be limited to what is strictly necessary. Further, the CJEU found that FISA 702 or E.O. 12 333, read in conjunction with PDD-28, does not grant the (European) data subjects rights actionable in the courts against the US authorities.

In other words this US legislation does not meet the proportionality requirements of EU law in the case of interference with fundamental rights, and the (European) data subjects do not have the right to an effective remedy, which are among the four essential European guarantees.

FISA 702 authorises the U.S. government to obtain information about "non-U.S. persons" that can reasonably be expected to be located outside the US for the purpose of collecting "foreign intelligence information".[16] This is done by issuing directives to electronic communications service providers to provide or arrange for the provision of personal data processed by the supplier.

CSPs are typically considered to be electronic communications service providers[17] and may therefore be subject to such directives under FISA 702.

For "U.S. persons" ("USP"), the term is defined in 50 U.S.C. § 1801(i) as:

> "A citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

In order to comply with the requirement only to collect information on non-USP's "reasonably believed to be located outside the United States", the relevant U.S. law enforcement authorities have developed targeting procedures.

Previous, declassified, targeting procedures show that when assessing the non-USP status of the target, the authorities examine information from their own and other agencies' datasets. However, it also appears that, in the absence of specific information regarding (i) the status of the target as a USP, (ii) whether the target is located outside the US, or (iii) in cases where the target's location is unknown, the authorities will presume that the target is a non-USP located outside the US.[18]

As Danish organisations will typically process information concerning non-USPs, it is the DDPA's immediate view that the use of CSPs located in the US by Danish organisations will normally fall within the scope of FISA 702 and thus be covered by so-called "problematic" legislation.

Consequently, you have two options if you wish to continue to use the CSP in question and transfer personal data to the US. You will have to either **(i)** implement supplementary to address this problematic legislation, or **(ii)** assess whether that legislation will be applied, in practice, with regard to the personal data you intend to transfer to the CSP.

In particular on supplementary measures

As a US CSP will generally fall within the scope of FISA 702, your first option is to implement supplementary measures in addition to the established transfer tool in the form of SCCs.

16 See 50 U.S.C. § 1881a.

17 As defined in 50 U.S.C. § 1881(b)(4).

18 NSA Targeting Procedures (2019): https://www.intel.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Targeting_17Sep19_OCR.pdf

In this context, you should note that contractual and organisational measures will generally not render ineffective access to personal data by US law enforcement authorities for surveillance purposes.[19] It will therefore be necessary to implement supplementary technical measures.

The EDPB's recommendations provide examples of supplementary technical measures you can implement as well as relevant cases detailing the implementation of such measures.[20]

The DDPA notes that these cases are only examples. As the controller you are free to implement other supplementary technical measures provided that you can demonstrate that the measures together with the transfer tool provide the data subject with an essentially equivalent level of data protection to that in the EU/EEA.

Among the examples of supplementary technical measures that are relevant when using cloud services are, in particular, encryption, pseudonymisation and so-called split processing.

If you use a cloud service where the CSP needs to have access to the transferred data in clear text, the EDPB cannot currently envisage supplementary technical measures that will effectively ensure an essentially equivalent level of protection to that in the EU/EEA.

Example 6

A Danish company wants to use a SaaS-service provided by a CSP in the US. The CSP is considered an electronic communications service provider and falls within the scope of FISA 702.

Therefore, the company considers that it is necessary to implement supplementary technical measures in addition to establishing a transfer tool in the form of the conclusion of SCCs.

According to the CSP's documentation, the personal data is encrypted when processed by the CSP. However, the company considers it appropriate to ask further questions about the implementation of this encryption.

The CSP specifies that the transmission of data to and from the CSP is encrypted ('in transit') and the data is encrypted when stored by the CSP ('at rest').

Upon the company's request, the CSP confirms that the data is not encrypted when the company's employees actively use the SaaS-service ("in motion").

In this case, the above-mentioned measures do not constitute effective supplementary technical measures since the CSP has access to the data in clear text when the company uses the SaaS-service.

Example 7

A Danish public authority wishes to replace its existing financial management system with a cloud-based system provided by a Finnish company.

19 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 53.

20 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraphs 79-97.

To deliver the system the company employs a cloud-based infrastructure provided by a global hyperscale public cloud provider. Additionally, the company has implemented technical measures in the form of IP address filtering so that the personal data processed in the system cannot be accessed from any IP addresses originating from outside the EU/EEA. This applies to data at rest, in transit and in motion. This type of measure is also known as 'geoblocking' or 'geofencing' and has traditionally been used to restrict access to websites and services to select countries.

It is clear from the contractual terms between the Finnish company and the CSP that personal data may be transferred to a large number of third countries *inter alia* in connection with the CSP's servicing and support of its infrastructure.

In this case, the above-mentioned measures do not constitute effective supplementary technical measures, since the company, as the CSP's customer, only has access to and control of its own infrastructure *i.e.* the financial management system developed by the company. Control of the underlying infrastructure remains with the CSP. It can therefore not be excluded that the CSP, when servicing its infrastructure, may have access to personal data contained in the financial management system from one or more third countries from which the infrastructure is provided.

It may also be the case that the authority, when reviewing the company's documentation, finds that the company has been aware of this issue and therefore employs dedicated infrastructure provided by the CSP that is technically separated from the CSP's other infrastructure. This is also supported by the contractual terms with the CSP which stipulate that the customer may opt in for dedicated infrastructure, which, however, entails a lower uptime guarantee, a higher price and fewer support possibilities – in other words, an "inferior" SLA for the customer.

Overall, in the latter case personal data will not be transferred to third countries at all and compliance with the requirements in Chapter V of the GDPR is not required.

Example 8

A Danish company has developed an application where users can register and monitor their blood sugar levels. The company is a small start-up and does not have the capacity to meet the upcoming high demand for the application expected by the company. For this reason, the company has hosted the application on the infrastructure of a hyperscale public cloud provider. The CSP guarantees that the data will be stored in the EU but cannot exclude that personal data will be transferred to third countries, *e.g.* in connection with service and upgrades of the infrastructure by sub-processors in the US.

As such, the company considers it necessary to implement supplementary technical measures in addition to establishing a transfer tool in the form of the conclusion of SCCs.

The company finds that encryption is the most appropriate supplementary measure and has taken the need for implementation of effective encryption into account early in the development process.

As a result, all communication is encrypted throughout the application across all servers where personal data is processed ("in transit").

In addition, the company has implemented encryption of the personal data in use ("in motion") and at rest ("to rest").

The company has entered into a distinct agreement with a specialised Swedish company who has implemented the encryption and manages the encryption keys. When the user inputs information in the application, the user communicates with the Danish

company via the Swedish processor where the relevant processing activities take place before the personal data is encrypted and forwarded to the US cloud provider for storage in the form of encrypted raw data. When the user wishes to read information in the application, the Swedish processor retrieves encrypted raw data from the CSP and decrypts the data and before passing it on to the user.

This is, in the view of the DDPA, an effective supplementary technical measure as the information is encrypted using keys stored in the EU, and the information is encrypted and only encrypted raw data is sent to and from the CSP in the US. The CSP does not have access to the personal data in clear text at any time – even when the user is actively using the application.

In particular on the practical application of the law

Alternatively, you may choose to transfer personal data to the US without implementing supplementary measures if you "have no reason to believe that the relevant and problematic legislation will be applied, in practice, to your transferred data or the organisation to whom you are transferring the data."[21]

As described above, CSPs in the US are typically considered to be electronic communications service providers and the use of such CSPs by a Danish organisation will generally fall within the scope of FISA 702.

The question then arises as to whether the specific data you wish to transfer will, in practice, fall within the scope of FISA 702 etc.

Under the surveillance programmes authorised under FISA 702, information on the targeted persons are collected by means of "selectors". Often highlighted examples of "selectors" are email addresses and telephone numbers.[22]

In addition, it follows from FISA 702 that the information which may be collected under the provision must be "foreign intelligence information"[23], which is defined as:

> "(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> (C) Clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defence or the security of the United States; or
> (B) the conduct of the foreign affairs of the United States."

Lastly, it follows from previous, declassified, targeting procedures with regard to "foreign intelligence purpose" that the authorities "reasonably assess, based on the totality of the circumstances [whether] the target is expected to possess, receive and/or is likely to communicate foreign intelligence information concerning a foreign power or territory". This assessment shall

21 EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 43.3.

22 U.S. Privacy and Civil Liberties Oversight Board's report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, p. 7.

23 See 50 U.S.C. § 1801(e).

be carried out by a specially trained staff member and shall be particularised and fact-based and informed on the basis of factual circumstances.[24]

With regard to "selectors", the DDPA has not been able to identify an exhaustive list of the types of "selectors" used by US law enforcement authorities.

As for the definition of "foreign intelligence information", the DDPA is of the view that the definition is broadly phrased, and a Danish organisation will generally – with few exceptions – not have the necessary prerequisites to assess the extent to which one or more types of personal data constitutes "foreign intelligence information". Therefore, this factor does not, in the DDPA's view, in itself contribute to the determination of the types of personal data which will be the subject of the surveillance programmes authorised under *inter alia* FISA 702.

Against this background, the DDPA is of the opinion that it will be difficult to document that the specific types of personal data that you wish to transfer to CSPs in the US will not be subject to the surveillance programmes authorised under *inter alia* FISA 702.

The DDPA does not exclude that there may be types of personal data which are not, in practice, subject to the surveillance programmes authorised under *inter alia* FISA 702. However, the DDPA expects that any controller who wishes to transfer personal data to CSPs falling within the scope of FISA 702 without implementing any supplementary technical measures can demonstrate, on the basis of objective, reliable and accessible information, that the specific types of personal data are not, in practice, subject to the surveillance programmes authorised under FISA 702.[25]

You may include the CSP's assessment in your documentation, but this assessment cannot stand alone and must be supported by objective, trustworthy and accessible information.

It is therefore insufficient to refer as evidence to your own or the CSP's subjective assessment that the transferred personal data cannot be targeted via "selectors" or is of no interest to US law enforcement authorities if that statement is not supported by objective, reliable, and accessible information, for instance from the authorities concerned.

Lastly, even if the specific personal data you wish to transfer effectively falls within the scope of the surveillance programmes authorised under *inter alia* FISA 702, you may still – without taking any additional action – transfer personal data to your CSP.

This presupposes, however, that your supplier, in practise, has not received any requests from US law enforcement authorities in the past, or that the types of personal data that you intend to transfer have not in any case fallen within the scope of such requests.

The DDPA notes that you must demonstrate that (i) the CSP is not prohibited from disclosing the existence of previously received requests as well as their scope, including with regard to the type of personal data covered by these requests.

It is also your responsibility as the controller to demonstrate that the types of personal data that you intend to transfer have not previously been in scope of any previous requests received by the CSP. This documentation must also be based on objective, reliable and accessible information, and not only on your own subjective assessment.

Example 9

A Danish company wants to use a SaaS-service provided by a CSP in the US.

24 NSA Targeting Procedures (2019): https://www.intel.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Targeting_17Sep19_OCR.pdf

25 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraphs 44-46.

The CSP is considered an electronic communications service provider and falls within the scope of FISA 702.

The CSP needs access to personal data in clear text for the provision of the service.

Given that neither email addresses nor telephone numbers will be transmitted, the company finds that the transferred data is unlikely to fall within the scope of the surveillance programmes authorised under FISA 702. However, the company's assessment is not supported by further evidence and is therefore based solely on the company's subjective assessment that this information may not, in practise, be targeted by US law enforcement authorities.

As the data is, in practice, not covered by "problematic" legislation, the company has not implemented any supplementary technical measures.

In this case, it would not be lawful for the Danish company to transfer the personal data to the US. This is due, in particular, to the fact that the company's assessment of whether the data falls within the scope of the surveillance programmes under FISA 702 is based solely on the company's own subjective assessment and not supported by additional objective, reliable and accessible information.

Example 10

A Danish company wants to use a SaaS-service provided by a CSP in the US. The CSP is considered an electronic communications service provider and falls within the scope of FISA 702.

The CSP needs access to personal data in clear text for the provision of the service.

The SaaS-service will only be used to process data that will be published on the company's website.

Although the data may formally fall within the scope of the surveillance programmes authorised under FISA 702, the main purpose of the surveillance programmes under FISA 702 is to obtain signal intelligence (SIGINT). Collection of publicly available information, on the other hand, is characterised as collection of open source intelligence (OSINT).

Having regard, in particular, to the fact that the data are intended to be made publicly available, the DDPA, in its immediate view, assumes that in practice such data will not, in practise, fall within the scope of the surveillance programmes authorised under FISA 702. The company may therefore lawfully use the SaaS service in question.

However, it should be noted that there may be processing of personal data, in particular in the back-end of the SaaS-service, which will not be publicly available and in theory and in practise fall within the scope of FISA 702.

Example 11

A Danish company wants to use a SaaS-service provided by a CSP in a third country. The company intends to transfer personal data to the CSP on the basis of SCCs. However, the CSP is subject to legislation in the third country which impinge on the effectiveness of the SCCs.

The CSP needs access to personal data in clear text for the provision of the service.

Having regard to the types of data that the company intends to process using the service and thus intends to transfer to the CSP, the company has assessed that the

specific data will not be subject to the legislation to which the CSP is subject in the third country in general.

The company's assessment is supported by declassified material from the third country's law enforcement authorities which exhaustively describes which types of data are subject to collection by the authorities under the relevant legislation to which the CSP is subject.

In this case, the DDPA considers that the company will be able to lawfully transfer personal data to the CSP without implementing supplementary technical measures, as the company can demonstrate that the data – based on objective, reliable and accessible information – is not subject to the problematic legislation in the third country.

Example 12

A Danish company receives health information from an American university hospital which relate only to US citizens. The company cleans the dataset of noise (methodical measurement errors), and the data is sent encrypted back to the American university hospital for use in patient care.

The company processes the data on behalf of the university hospital as a processor, and the company is subject to data protection law by virtue of its establishment in Denmark. The company's "re-export" of data to the American university hospital is therefore in scope of Chapter V of the GDPR.

As a transfer tool the company has entered into the SCCs with the American university hospital. Additionally, the company has assessed the legislation and practices to which the university hospital is subject and concludes that the university hospital is generally covered by legislation which impinges on the effectiveness of the concluded SCCs. However, in its assessment the company's also finds that the relevant legislation does not apply to data on US citizens. This assessment is supported by a report from a recognised American university.

In this case, the DDPA is of the opinion that the Danish company can "re-export" the data as the company has (i) established a transfer tool and (ii) documented that the legislation to which the university hospital is subject – although problematic in itself – is not applied in practice to the data transferred to the university hospital and the company's assessment is supported by objective, reliable and accessible information.

Example 13

A Danish company uses a CSP based in the EU for hosting its CRM system. The CSP is a subsidiary of a US parent company.

According to the data processing agreement, the CSP processes certain types of metadata which are personally identifiable for its own purposes (such as capacity planning, security management and service improvements), including transfers the data to its US parent company.

The CSP is considered a controller for its processing of the data for the above-mentioned purposes and is therefore itself responsible for complying with Chapter V of the GDPR in respect of its transfer of the data to the US.

Note that in this case, prior to engaging the CSP for the processing activity, the Danish company must assess on which legal basis it may disclose the relevant metadata to the CSP for the CSP's processing of the data for its own purposes.

3.6 Processing carried out within the EU/EEA by companies which may face requests from authorities in third countries

In cases where a CSP processes personal data solely within the EU/EEA, including using only sub-processors in the EU/EEA, you are, in principle, not required to comply with the rules in Chapter V of the GDPR.

However, CSPs established in the EU/EEA may, for instance due to their group structure, receive requests from law enforcement authorities in the third country where the CSPs' parent companies are established.

For instance, for CSPs whose parent company is established in the United States this could be the case for requests under the US CLOUD Act.[26]

It is not in itself unlawful to use a CSP whose parent company is subject to laws in its country of establishment that give law enforcement authorities the competence to request information held by other group members, including those in the EU/EEA.

For clarification of the issue see the example below cited from the DDPA's guidance on transfers to third countries.[27]

In particular on disclosure of personal data upon request from authorities of third countries

A processor may process personal data, including transfer the data to third countries, only to the extent that the controller has instructed the processor to do so or where required by EU or Member State law.

However, where a processor in the EU/EEA is also established in a third country, the processor may in some cases receive requests from the authorities of that third country for the disclosure of personal data processed by the processor on behalf of the controller.

If the processor elects to transfer personal data to the third country in contravention of the controller's instructions, the transfer shall be considered as "unintended" on part of the controller, which means that the controller is not obligated to comply with the provisions on transfers to third countries.

However, the controller must be aware of a number of issues in this regard:

- Firstly, the controller may only use processors that can provide sufficient guarantees to comply with data protection law. In this context, the controller should ask the processor to clearly indicate whether the processor is subject to laws of third countries which – despite the controller's instructions to the contrary – may require the processor to disclose personal data processed in the EU/EEA to authorities in third countries.

- Secondly, the controller must ensure the necessary security of processing, including that the processor ensures the confidentiality of the processed personal data and does not make it accessible to unauthorised persons. In doing so, the controller must carry out a risk assessment in order to assess which measures the controller should implement to ensure such confidentiality.

26 The DDPA is aware that it has been argued that other US legislation, including FISA 702, is also considered to have an extraterritorial effect in the same way as the US CLOUD Act. However, it is currently the opinion of the DDPA that it has not been established in practice whether, and to what extent, FISA 702, among others, has an extraterritorial effect.

27 The DDPA's guidance on transfers to third countries, p. 11.

- Thirdly, the controller must audit its processor. Where the controller becomes aware that the processor is acting in breach of the data processing agreement by transferring personal data to a third country in contravention of the controller's instructions of the controller, the controller shall take immediate action to address this.

It should also be noted that where processor acts in breach of the controller's instructions by transferring personal data to an authority in a third country and thus itself determines the purposes and means of the processing, the processor is considered to be a controller in respect of that processing.

As per item 2 in the above-mentioned example, the present issue is, in the opinion of the DDPA, a matter of appropriate security of processing where you as the controller must ensure *inter alia* the ongoing confidentiality of the data.

In this context, you should be aware that if your European CSP as your processor complies with a request from law enforcement authorities in a third country, it is considered a personal data breach on part of the controller as an unauthorised disclosure of personal data to the concerned law enforcement authority will have occurred.

However, it should be stressed that this question of an appropriate level of security of processing is limited only to cases where the use of the CSP does not otherwise involve any intended transfers of personal data to third countries, including in relation to the provider's servicing of its infrastructure, the provider's provision of support of your cloud service, the provider's access to its infrastructure for the purposes of capacity planning etc.

Example 14

A Danish company wants to use a cloud service from a US CSP to send out newsletters.

In this context, the company will process, in particular, data concerning the data subjects' email addresses as well as information concerning the newsletters that have been sent out.

The service is provided by a European subsidiary on the basis of infrastructure located exclusively within the EU/EEA. Consequently, there will be no intentional transfers of personal data to third countries.

In this case, the US CSP is subject to the US CLOUD Act which provides that a CSP may be required to *"preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."*

Personal data processed by a European subsidiary of a US CSP is typically considered to be under the US parent's "possession, custody, or control".

As part of its general risk assessment concerning security of processing, the company has assessed the risk to data subjects stemming from possible disclosure of personal data to US law enforcement authorities:

- Probability: In its Transparency Reports the CSP has stated that it annually responds to a number of requests under the US CLOUD Act. Against this

background, the company has assessed that it is LIKELY (4)[28] that the CSP will comply with a request under the US CLOUD Act.

- Severity: Having regard to the type of personal data that will be processed using the cloud service, it is the company's assessment that the potential consequences for the data subjects in US law enforcement authorities receiving data relating to their email address and which newsletters they have received will be an experience of stress and mistrust/fear. As such, the severity of the incident would be LOW (2).

Consequently, the company has established that the overall risk for data subjects in the possible disclosure of personal data pursuant to a request under the US CLOUD Act is MEDIUM (8).

Against this background, the company engages in dialogue with the European CSP with a view to include in the terms of their agreement that the CSP, including the US parent, shall, to the greatest possible extent, challenge any disclosure requests under US law.

The company considers that this amendment to the parties' agreement constitutes an appropriate organisational security measure that reduces the likelihood of US law enforcement authorities actually receiving personal data under a US CLOUD Act request to an UNLIKELY (2) level. Accordingly, the company considers that the residual risk for the scenario is LOW (4).

In this case, the company will have implemented appropriate security measures with regard to the specific threat and met its obligations under the provisions on security of processing.

28 In the example, the DDPA has based its assessment criteria of the evaluation of both probability and severity on a scale of 1-5.

Guidance on the use of cloud

Published by:
The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk