English summary of Kahn Pedersen's report 2020:3

kahn pedersen

Public cloud services for private businesses in Sweden

– A legal analysis and introduction to the Folke© Methodology

DISCLAIMERS

This report is an English translation of the original Swedish version. The translation may contain errors or incorrect use of the English language. Please contact Advokatfirman Kahn Pedersen at info@kahnpedersen.se if you suspect any incorrect or misleading language and/or if you have other questions related to the report.

Please note that this report does not constitute legal advice under any circumstances. Any and all direct or indirect liability for the content of this report (and/or for reliance thereon) is hereby explicitly disclaimed. We strongly encourage you to seek legal advice regarding any legal issue or scenario related to cross-border transfers of personal data from the EU and/or related to use of public cloud services. This report is not a complete description of the legal issues associated with public cloud services.

All statements made in the report are based solely on Swedish and EU law. Where a cloud provider or its subcontractors are based in a foreign jurisdiction, local legal counsel should always be engaged. Furthermore, it should be noted that this report only considers and takes into account those legal areas and issues that are expressly covered in the report. We cannot rule out the possible relevance of other legal areas or issues in a particular case.

Lastly, please note that the conclusions in this report are based on typical circumstances, conditions, and risks that are normally associated with the use of cloud services provided by global cloud providers. Neither this report nor the Folke© Methodology can or will replace the need for careful legal assessment in each case.

1. Introduction

1.1 Why a Report on Public Cloud Services?

"*There is no cloud, it's just someone else's computer*" is a well-known assertion made regarding so-called cloud services. We would argue that this statement is actually both correct and incorrect. It is correct in the sense that cloud services are typically based on shared computer resources and infrastructure located in data centers under the control of a cloud services provider (rather than under the sole control of the cloud customer). The statement is also incorrect, since it implies that cloud services are nothing new, and thus diminishes the importance, and disruptive nature, of cloud services as has been evident for the past 10 to 15 years.

Cloud services are used by almost all organizations in Sweden, in some capacity and to some extent, across all industries. A common misperception is that the only public cloud services available are provided by US hyperscalers. Although US cloud providers indeed dominate the market, it is important to note that there are several public cloud providers in the EU, as well as domestic alternatives. In particular, the EU is investing significant resources in the Gaia-X initiative.[1]

By definition, the use of any public cloud service will involve transfer/migration and storage of the cloud customer's data. When the cloud provider is based in a different jurisdiction than the cloud customer and/or is otherwise subject to laws and regulations other than those governing the cloud customer, a number of issues and legal risks arise related to data protection, trade secret protection, and conflict of laws. This situation creates a rather cumbersome burden for each cloud customer in terms of making in-depth and comprehensive assessments of the legal, regulatory, and technical implications of each public cloud service being considered.

Recently, the legal complexities surrounding the use of public cloud services have become even more apparent due to the ruling of the Court of Justice of the European Union ("**CJEU**") in case C-311/18 ("**Schrems II**").[2]

The purpose of this report is to share our views and to present certain methods and approaches that we have found useful when navigating the current legal landscape. Specifically, the primary focus is legal risk assessment related to cloud migration to US hyperscalers.

We hope and trust that this report can serve as a contribution to the ongoing legal discourse on the use of public cloud services. We also hope that the report could serve as a practical and useful guide in

1 See https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

2 Judgment of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 ECLI:EU:C:2020:559.

connection with contemplated cloud migration and digital transformation initiatives.

1.2 We apply a Risk-Based Approach

Our approach to the use of public cloud services is based on three general and overarching principles. Firstly, we have concluded that the use of public cloud services is not illegal or otherwise prohibited in general – at least not in Sweden. Secondly, we believe that new technology and delivery models should, at least as a starting point, be allowed unless expressly prohibited by law. Thirdly, we believe that the method used in the General Data Protection Regulation ("**GDPR**")[3], i.e. a risk-based approach, is necessary to make informed decisions related to cloud migration.

The third and final principle is particularly critical for this report. In our view, it is possible for a particular public cloud service to be considered lawful and appropriate for use in one use case while being unlawful and inappropriate for use in another use case.

A meaningful due diligence review of the lawfulness and appropriateness of adopting public cloud services will require a comprehensive and nuanced risk assessment in which many different strategic, technical, legal, regulatory, and commercial risks are weighed against each other.

A specific legal issue relates to whether Article 46 of the GDPR, the Schrems II case, and the European Data Protection Board's ("**EDPB**") draft recommendation on supplementary measures (see further in Section 2 below) can support a risk-based approach to cross-border data transfers to a 'third country'. Is it, for example, possible to consider the sensitivity of the particular data sets that would be subject to such data transfer, or what the implications of a potential unauthorized disclosure (as defined in Section 1.3 below) would be for the data subjects?

On the one hand, it seems clear that the Schrems II ruling and the EDPB's draft recommendation do not explicitly support adopting a risk-based approach on this particular issue. On the other hand, a risk-based approach would be in line with Articles 5(1)(f), 24, and 32 of the GDPR as well as the general EU law principle on proportionality (cf. Article 47 in the EU Charter). Another aspect is that an absolute prohibition on cross-border data transfers to third countries which do not have essentially equivalent data protection laws (without risk assessment) could potentially be in conflict with international trade policies and treaties.[4]

---

3 EU Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

4 See, e.g., https://www.europeanpapers.eu/en/europeanforum/issue-of-data-protection-in-eu-trade-commitments. The relationship between Schrems II and Convention 108 issued by the Council of Europe is another interesting trade issue; see https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb.

Achieving an absolute or perfect level of security or data protection is unrealistic in practice. For our clients in the private sector, doing business will always involve risks, no matter the industry or jurisdiction. Some risks will be commercial, others will be operational, and some will relate to compliance with legal requirements.

Our general approach is that a prudent and diligent private sector cloud customer should strive to: (1) identify and isolate all potential risks connected to cloud migration (including but not limited to data protection); (2) implement available and appropriate risk mitigation measures (see further in Section 3 below); and then (3) assess and evaluate residual risks (if any). The question of whether the residual risk is acceptable is not a legal decision. It is – and should be – a strategic business decision for the cloud customer.

To this end, we have developed a model for legal risk assessment in connection with cloud migration – the Folke© Methodology – which we are proud to present in this report. This method is intended as a dynamic tool for visualizing how contractual, technical, and strategic choices will affect the overall risk assessment related to cloud migration.

1.3 Some Key Definitions

Throughout this report, we use the concepts of "risk", "jurisdictional risk" and "unauthorized disclosure". Understanding these concepts, and how we use them, is critical when reading this report and using the Folke© Methodology.

We use the standard definition of "risk", meaning that risk is calculated by multiplying (i) the likelihood of an event occurring by (ii) the severity of the consequences from the event occurring.

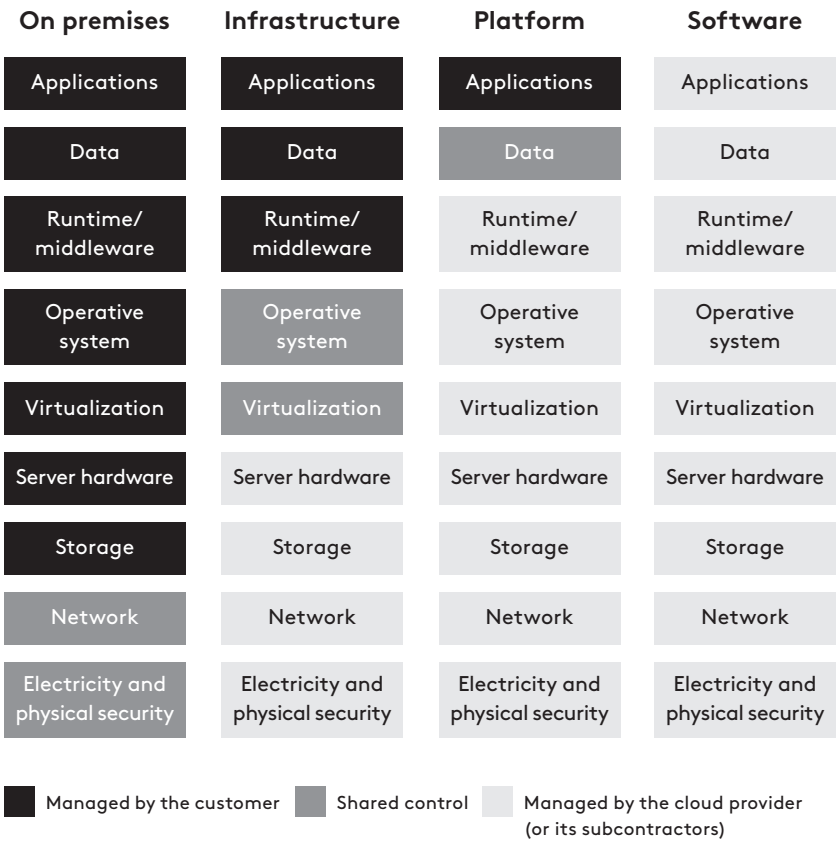
The type of event which is evaluated in this report is a cloud provider's voluntary or compulsory disclosure of customer data/information (or another processing activity as unilaterally decided by the cloud provider or a governmental authority having jurisdiction over the cloud provider) *in compliance with* certain laws, regulations, or contractual terms applicable to the cloud provider which, at the same time, is *in conflict* with other laws and regulations that apply to the controller/owner of the data (i.e. the cloud customer). In this report, we call this kind of disclosure an "unauthorized disclosure" by the cloud provider, and the risk of a potential unauthorized disclosure is referred to as "jurisdictional risk".

1.4 An Overview of Public Cloud Services

Public cloud services are typically divided into "Infrastructure as a service" ("**IaaS"**), "Platform as a service" ("**PaaS**"), and "Software as a service" ("**SaaS**"). Common to all such as-a-service categories is

that an external service provider (the "cloud provider") will – to some extent and in many different ways – be entrusted to host or process the cloud customer's data.

The key differences between an IaaS, a PaaS, and a SaaS can be illustrated in the following table, where these services are also compared to an IT service where customer itself will manage all layers (so-called "on premises"):



It is essential to understand the nature and category of a specific public cloud service in order to be able to interpret and apply the legal frameworks which are relevant when assessing and advising as to whether the particular cloud service could, and should, be used by the cloud customer.

Generally, an IaaS and a PaaS are easier to customize and tailor to a customer's individual needs, since such services can be used and deployed in many different ways, leveraging specific and tailored risk mitigation strategies and technical security measures. In comparison, a SaaS does not allow the same level of customization and will often be provided on contractual terms and with technical/deployment setup options with no substantial scope for negotiation. In this respect, an IaaS and a PaaS clearly place the cloud customer in a better position to maintain control over their data and to decide on implementation of key technical and organizational security measures.

It should also be noted that many SaaS providers are, in fact, using third party IaaS or PaaS providers. This means that a SaaS provider may very well be reliant on other cloud providers, which means that a cloud customer cannot take for granted that a particular SaaS provider will have exclusive control over the data in their own SaaS service. Any due diligence review of a SaaS provider will therefore need to include review of underlying IT infrastructure, including additional third-party IaaS/PaaS providers.

PART I

2. Jurisdictional Risk, GDPR, Schrems II, and Data Transfers to the US

2.1 US Cloud Providers and Jurisdictional Risk

Discussing jurisdictional risk in relation to global cloud providers is nothing new. The risk is relevant not only in regard to US cloud providers – it must be considered for all cross-border data transfers to any location outside of the EU. For example, jurisdictional risk must be assessed when using IT support functions in India or when engaging software developers from the Ukraine or China.

Jurisdictional risk has, however, been the subject of intense scrutiny in recent years, particularly related to US cloud providers. This is mainly due to the broad use and adoption of public cloud services along with the considerable market share by US-based or US-owned corporations. Another reason for the legal debate surrounding US cloud services is known US government surveillance programs, not in the least the US intelligence materials disclosed by Edward Snowden in 2013.

The adoption of the CLOUD Act[5] by the US in 2018 further increased the legal discussions related to jurisdictional risk regarding US cloud providers. In short, the CLOUD Act gives US law enforcement authorities the right, under certain circumstances, to request disclosure or access to data hosted by US cloud providers, even if the data is stored outside the US (see further below).

On 16 July 2020, the CJEU published a landmark ruling in the Schrems II case. For the purposes of this report, the key aspects of the Schrems II case are that:

1. the CJEU ruled that the Standard Contractual Clauses ("**SCC**") issued by the European Commission remain a valid and legal mechanism to transfer data to a third county[6];

2. the CJEU stated that US surveillance laws, such as the Foreign Intelligence Surveillance Act ("**FISA**") Section 702 and Executive Order 12333 ("**EO 12333**"), mean that cloud providers that fall under

5 Clarifying Lawful Overseas Use of Data Act (H.R.4943).

6 Schrems II, p. 149.

US jurisdiction are generally unable to ensure a level of data protection which is "essentially equivalent" to the EU law[7];

3. the CJEU clarified that an EU cloud customer relying on the SCCs to transfer data to a third country needs to verify, on a case-by-case basis, whether the law of the third country of destination ensures adequate protection under EU law and, where necessary, identify and implement "supplementary measures" in order to rely on the SCCs[8];

4. the CJEU ruled that if sufficient "supplementary measures" cannot be identified or implemented, then the EU cloud customer is essentially not able to legally transfer personal data to the US in compliance with the GDPR.[9]

After the Schrems II case, the EDPB adopted a draft version of recommendations concerning third country data transfers and supplementary measures for such transfers (the "**Draft Recommendations**").[10] In particular, the Draft Recommendations set out seven different use cases for public cloud services and the EDPB's assessment is that effective supplementary measures can be implemented in only four of these. All four of these use cases relate – in our opinion – to rather obscure usage of cloud services that do not leverage the strengths of public cloud platforms. This means that the Draft Recommendations provide very limited scope for European businesses to use US public cloud services in compliance with the GDPR. Please see further below in section 3.3.

Final recommendations from the EDPB are expected in mid-2021.

2.2 MLATs and Extraterritorial Legislation (the CLOUD Act situation)

Disclosure of personal data and other information to foreign governments has, for quite some time, been possible and legal for a variety of reasons, including for purposes of law enforcement. Traditionally, such disclosures have been subject to an agreed procedure and international agreement concerning how to manage such enquiries and data disclosures, primarily through bilateral or multilateral mutual legal assistance treaties ("**MLATs**").

However, the adoption of the CLOUD Act in the US establishes a completely different legal procedure, whereby US governmental authorities can unilaterally obtain information stored in another jurisdiction,

7 Schrems II, pp. 184-185.

8 Schrems II, p. 133 and p. 184-185.

9 Schrems II, p. 136.

10 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted – version for public consultations. Available at https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

provided that such information is in the "possession, custody or control" of a US entity.

The CLOUD Act is intended to clarify the extraterritorial nature of another piece of US legislation, namely the SCA[11]. Similarly, the CLOUD Act clarifies that the SCA can be invoked by US law enforcement agencies despite the absence of an MLAT or other international agreements.[12]

When information requested by a US law enforcement agency includes personal data, a US data processor or sub-processor (such as a cloud provider) will, effectively, be obligated to disclose personal data to US government authorities without legal basis under Swedish and EU law. In fact, this is the very definition of unauthorized disclosure as used in this report.

To further complicate things (from an EU/GDPR perspective), a disclosure order under the CLOUD Act can be subject to a gag order from a US court, prohibiting the US cloud provider from notifying or informing the customer of the request or that a disclosure has taken place.

The aforementioned means that there is an ongoing, inherent, and unresolved conflict of laws between Swedish and EU law and the CLOUD Act.[13] However, it is important to note that US governmental authorities' ability to access data under the CLOUD Act is not unlimited. The CLOUD Act includes a number of relevant limitations as to what data that can be requested, including for example:

- requested data must relate to a current investigation subject to US jurisdiction (i.e. no "fishing expeditions" for data);
- only data that the cloud provider has control over at the time of the request can be covered by a request;
- the US authority cannot ask the cloud provider to store more, or other, data than the cloud provider would normally store in the ordinary course of providing its service;
- the US authority cannot ask the cloud provider to modify its service or IT system, and/or to transfer the data from one server to another; and
- a request must be limited and precise in scope. The US authority must specify whom it concerns, what type of data it concerns, the geographical location where the data is stored and during what time the relevant data have been uploaded or collected by the cloud provider.

---

11 Stored Communications Act (Title 18 of the United States Code, Chapter 121, §§ 2701–2712).

12 It should be noted that the CLOUD Act anticipates new bilateral agreements, so-called Executive Agreements, between the US and other jurisdictions. Such Executive Agreements are not, however, a prerequisite for US governmental agencies to request and obtain data under the CLOUD Act.

13 See https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

2.3 FISA Section 702 and EO 12333 (the Schrems II-situation)

Section 702 of the US FISA legislation enables the US Attorney General and the Director of National Intelligence to jointly give permission to surveil non-US citizens outside the US in order to collect data from foreign intelligence. Such permission may be given on condition that the US Foreign Intelligence Surveillance Court ("**FISC**") gives its approval in advance. However, the Privacy Shield Decision states that the FISC does not approve individual surveillance measures. The FISC primarily approves surveillance programs that, in general, do not contain data about individuals but, instead, include categories of foreign intelligence. This constitutes legal ground for surveillance programs such as *Prism*[14] and *Upstream*[15].[16]

Executive Order 12333 allows the US National Security Agency ("**NSA**") to gain access to data that is "in transit" to the US, since the NSA has access to underwater cables on the floor of the Atlantic. The NSA is accordingly, without legislative regulation, able to collect and store data before it arrives in the US, where such data is covered by FISA.[17]

FISA Section 702 and EO 12333 were the primary focus of the CJEU in the Schrems II ruling in its review of current US legislation. It is clear that the impact of these laws needs to be carefully assessed by any EU cloud customer. However, finding effective safeguards and strategies to protect against the implications of FISA Section 702 and EO 12333 is often very difficult in practice (see Section 3 below).

2.4 Relevant Provisions in the GDPR

When engaging a US cloud provider, there are, mainly, three articles in the GDPR that could potentially be breached.

- Principle of lawful processing (Article 5(1) of the GDPR). Disclosure of personal data to foreign authorities in conflict with the GDPR is not lawful. The processing is also unlawful if a data controller transfers or discloses personal data to someone whom it can *reasonably assume* will not process the data in a GDPR-compliant manner. This Article should not, in our view, prohibit the engagement

14 Within the framework of the Prism program, the providers of Internet services, according to the findings of the referring court, are obliged to provide the NSA with all communications sent and received by a "selector", whereby some of these messages are also transferred to the FBI and CIA.

15 Regarding the Upstream program, the referring court found that the telecommunications undertakings operating in the "backbone" of the internet – that is, the cable network, switches, and routers – are required to allow the NSA to copy and filter the traffic flows on the internet in order to collect communications sent to or received by or concerning a non-US citizen that has been brought to the attention by a "selector". According to the referring court, the NSA has access, within the framework of the Upstream program, to both metadata and the content of the communication concerned.

16 See Schrems II, pp. 179-181.

17 See Schrems II, p. 63.

of a processor (or approval of a sub-processor) under US jurisdiction *per se*. Rather, this issue should be a part of the cloud customer's risk assessment related to the public cloud service.

- Prohibition against transfers and disclosures not authorised by European Union laws (Article 48 of the GDPR). Disclosure of personal data to a non-EU governmental authority must comply with Article 48 of the GDPR. On this topic, the European Data Protection Supervisor ("**EDPS**") and the EDPB have published a joint statement regarding the CLOUD Act and its relationship to the GDPR. They argue that disclosure of personal data about an EU citizen in accordance with the CLOUD Act must be based on an MLAT or another international agreement in order to be compliant with the GDPR. In the absence of such an international agreement, the disclosure can only be legal in the event of exceptional circumstances and where such disclosure is necessary in order to protect vital interests of the data subject. If a cloud provider (typically a data processor) receives a disclosure order from a governmental authority, such disclosure will be the cloud provider's responsibility, rather than the cloud customer's (typically a data controller).

- "Sufficient guarantees" from a data processor (Articles 28(1) and 28(4) of the GDPR). Every cloud customer is obligated to ensure that its cloud provider(s) are able to, and will, provide *sufficient guarantees* to implement appropriate technical and organizational measures. If the cloud customer is aware that a cloud provider is in fact unable (e.g. due to US laws) to comply with the GDPR, then the cloud customer (as data controller) should, arguably, be held responsible for not having examined the processor sufficiently and for not ensuring sufficient guarantees in the cloud contract (data processing agreement).

Furthermore, when transferring personal data to a third country (or permitting a cloud provider to transfer such data), the cloud customer also needs to take the following into account.

- Article 44 regarding the general principle of transfers. Third country transfers must have a legal basis/mechanism in the GDPR.

- Article 45 regarding transfers based on adequacy decisions. A limited number of third countries have been considered to have data protection laws that provide protection for the personal data of EU citizens equivalent to the protection under the GDPR.[18] Transfers of personal data to those countries are compliant with the GDPR. On this point, it should be clarified that the US currently does not have a valid adequacy decision.

- Article 46 regarding appropriate safeguards. If a third country does not have an adequacy decision, additional safeguards are

18 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

required in order for the transfer to be compliant with the GDPR. Such safeguards are, for example, SCCs and Binding Corporate Rules together with, where applicable, supplementary measures as per Schrems II.

- Article 49 regarding derogations for specific situations. In the absence of an adequacy decision pursuant to Article 45(3) or appropriate safeguards pursuant to Article 46, a transfer of personal data to a third country may take place in specific situations, for example if the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

3. Are US Public Cloud Services Compliant with the GDPR?

3.1 Cloud Due Diligence Review

Exposing personal data and other customer data to the jurisdiction of the US legal system entails a significant level of jurisdictional risk. Does this mean that such public cloud services are noncompliant with the GDPR? In many cases, the answer is yes. In certain other cases, the answer is no.

Jurisdictional risk will arise immediately upon data transfer/access to a cloud provider in the US, not when the cloud contract is signed or when the data is, in fact, disclosed by the cloud provider to a non-EU governmental authority. A diligent cloud customer based in the EU must perform a comprehensive analysis and review prior to[19] adopting or migrating to any public cloud service (regardless of whether it is an IaaS, a PaaS, or a SaaS). It is important to remember that storage of data at rest within the EU does not completely mitigate the inherent risk of unauthorized disclosure of customer data resulting from extra-territorial legislation in a third country such as the US or China.

In other words, we believe that the GDPR (and perhaps other legal frameworks as well, see further below in this report) includes – at the very least – a requirement that a cloud due diligence review must be performed for all non-EU public cloud services. This requirement includes, but cannot be limited to, performing a data protection impact assessment pursuant to Article 35 of the GDPR.

3.2 Data Protection Impact Assessments under the GDPR

A cloud customer is typically required to perform a Data Protection Impact Assessment ("**DPIA**") per Article 35 of the GDPR before using a public cloud service. The main purpose of a DPIA is to assess what technical and organizational security measures that are "appropriate" as per Articles 24 and 32 of the GDPR.

Article 35 of the GDPR presents three scenarios where it is mandatory to perform a DPIA:

19 If a particular cloud customer intends to sign a cloud contract without having completed (and documented) its cloud due diligence, we would generally advise adding successful cloud due diligence review as a condition precedent in the relevant cloud contract.

- in the case of systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

- in the case of processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

- in the case of systematic monitoring of a publicly accessible area on a large scale.

The GDPR also includes a number of exceptions from the obligation to conduct an impact assessment, for example if an impact assessment has been conducted recently by the controller for a similar processing.

In addition, the Swedish Authority for Privacy Protection (*Sw. Integritetsskyddsmyndigheten*) has presented a list of nine different factors to determine whether a DPIA is required.[20] If two or more of these factors apply for the intended processing activity, a DPIA is required. In relation to public cloud services, the most relevant factors are:

- processing on a large scale;

- processing of special categories of data or data of very personal characteristics;

- processing regarding persons in a dependent or disadvantaged position; and

- usage of new technology or new organizational solutions.

Identified data protection risks are commonly ranked for probability and severity using the following risk categories: 1. Negligible; 2. Limited; 3. Significant; and 4. Maximum. There are several different methods and templates for performing DPIAs, for example a software-based application developed by the French Data Protection Authority, CNIL.[21]

3.3 Use Cases in the EDPB's Draft Recommendation

The Draft Recommendations introduce a six-step-procedure to guide data exporters (meaning, in this case, cloud customers) to map their transfers, assess appropriate transfer mechanisms for the transfer,

20 Swedish Authority for Privacy, List regarding Data Protection Impact Assessments according to Article 35(4) of the Data Protection Regulation, 16 January 2019, journal no. DI-2018-13200, https://www.imy.se/globalassets/dokument/beslut/list-regarding-data-protection-impact-assessments.pdf.

21 https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

the level of protection for personal data in the third country as well as which supplementary measures that need to be adopted to ensure appropriate protection for personal data before the transfer is conducted and re-evaluate such assessments at appropriate intervals.

According to the EDPB, data "in the clear" cannot be made available to a cloud provider in a third country that does not have "essentially equivalent" data protection laws to those within the EU. The Draft Recommendations present seven use cases where the EDPB elaborates on supplementary measures and under which circumstances they can ensure appropriate protection for personal data:

- Use Case 1: Storage of personal data for back-up purposes or other purposes that do not require the cloud service provider to have access to data in the clear. In this use case, strong encryption, where the cloud provider does not have access to encryption keys, can constitute effective supplementary measures.

- Use Case 2: Correctly pseudonymising personal data before transferring it to a third country constitutes effective supplementary measures. In our opinion, correct pseudonymization requires that only the data exporter, i.e. the cloud customer, has access to information for attributing personal data to a specific data subject and not the cloud service provider (i.e. data importer).

- Use Case 3: Personal data is only transiting a third country when transferred to a country with an adequate level of protection. In this use case, strong encryption, where the cloud provider does not have access to encryption keys, can constitute effective supplementary measures.

- Use Case 4: Transfers to a service provider in a third country protected by that country's law, i.a. for jointly providing medical treatment or legal services. In this use case, strong encryption, where the cloud provider does not have access to the encryption keys, can constitute effective supplementary measures.

- Use Case 5: Split or multi-party processing of personal data by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. If the data, prior to transmission, is split in such a way that no individual processor receives suffices to reconstruct the personal data in whole or in part, the split is considered as an effective supplementary measure.

- Use Case 6: This use case is, in short, relevant for the use of most SaaS and other cloud services where the cloud provider requires access to personal data in the clear for processing. In this use case, the EDPB found no effective supplementary measures.

- Use Case 7: This use case is, *inter alia*, relevant where a service provider in a third country is permitted to have direct access to

personal data for shared business purposes, for example to enable the service provider to offer customer support services to data subjects via e-mail or phone. In this use case, the EDPB found no effective supplementary measures.

For use cases 6 and 7, which are relevant for many cloud services, EDPB is unable to envision effective technical measures that would properly protect the data subjects' rights under the GDPR. It is also noteworthy that EDPB finds that encryption during transit and encryption of data at rest cannot guarantee an essentially equivalent level of protection for personal data, if the cloud service provider will have access to unencrypted data in order to be able to provide its services and has the cryptographic keys in its possession.

However, in regard to use case 6, EDPB does not rule out that further technological development might offer measures that achieve the business purposes, without requiring access to personal data in the clear.

3.4 Other Potential Technical Security Measures in the Cloud (Examples)

Ensuring appropriate technical and organizational security measures in the cloud is a complex endeavour. This is clearly indicated by the Draft Recommendation, which includes rather detailed and strict requirements related to pseudonymization and encryption in order to transfer data to a third country (see previous section).

Based on the Draft Recommendation, there is in practice little room for legal transfers of personal data to the US and other third countries without data protection laws that are "essentially equivalent" to those within the EU. However, there are still additional security measures that should be considered in this context – bearing in mind that such measures may not meet EDPB's threshold of being legally "effective".

Generally, we deem that the following non-exhaustive measures might potentially mitigate jurisdictional risk depending on the circumstances in each individual case. Please note that the relevance and effectiveness of the measures below also vary depending on whether the transfer relates to the circumstances described in section 2.2 or section 2.3 above:

- ensuring that the data is stored at rest within the EU/EEA only;

- implementing additional contractual measures as those set out in the Draft Recommendations,[22] including an obligation for the cloud service provider to review the legality of any order to disclose data and to challenge the order where legally possible;

22 See Annex 2, "Additional contractual measures" in the Draft Recommendations.

- limiting the types of data in the cloud service, e.g. by excluding the most sensitive data types;

- limiting use of the cloud services, e.g. by only processing data in memory/use in the cloud;

- implementing all available options and offerings from the cloud provider related to encryption and pseudonymization (e.g. confidential computing);

- adding further security functions in or to the cloud service, such as mobile/laptop device management to be able to cut off access from certain devices;

- implementing robust exit and continuity plans to ensure the possibility of swift relocation of workloads to another provider;

- creating internal policies and guidelines on how to use the relevant cloud services;

- limiting the use of the cloud provider's support function (if possible and relevant); and

- setting up internal functions and controls to follow the changes of the legal situation in the EU and in relevant third countries.

4. Additional Legal or Compliance Considerations for Certain Sectors

4.1 Swedish Authorities and Other Public Entities and Bodies

There are a number of additional factors that authorities and other public sector entities or bodies must take into consideration before entering into any public cloud contract.

Most crucially, it is necessary for such entities to assess the Public Access to Information and Secrecy Act (2009:400) ("**PAISA**") and, specifically, whether and under what circumstances the use of public cloud services will give rise to an undue disclosure (*Sw. röjande*) under the PAISA. However, neither this particular issue nor any other public sector-specific legislation or regulation fall within the scope of this report.

4.2 Operations under the Swedish Protective Security Act

The purpose of the Swedish Protective Security Act (2018:585) ("**SPSA**"), is to, protect Sweden from espionage, sabotage, terrorist offences and other crimes that may threaten operations covered by the SPSA, and otherwise protect classified information, by implementing proactive measures. A fundamental principle of the SPSA is that the objects and interests worthy of protection shall have the same level of protection regardless of where the data is processed or the operation is carried out or by whom. The protection for such objects and interests shall therefore not deteriorate if an external service provider is engaged.

SPSA is applicable to anyone, i.a. a private company, government agency or municipality, conducting operations that are of importance for the safety of Sweden, or are covered by an international protective security commitment that is binding for Sweden (security-sensitive activities), regardless of its legal form. In order to ensure that the purposes of the law can be fulfilled, even when society or threat scenarios change over time, the types of operations covered are not exemplified or summarized in any way, as they might vary over time. Therefore, it is only stated that SPSA is applicable on operations where potential information disclosure could be detrimental to the national security of Sweden.

Cyberattacks are considered to be one of the most serious threats against Swedish national security. Such attacks are often targeted at

service providers in order to take control over authorities or companies. Consequently, operations covered by SPSA who wish to engage a cloud service provider must assess whether the cloud service provided can be used in accordance with SPSA, what risks such use can entail and which measures must be implemented to protect the national security of Sweden, as well as comply with far-reaching safety and security requirements. To make these assessments, entities covered by SPSA must get sufficient information regarding the cloud service provider, which can be hard to obtain with regards to a foreign cloud service provider, including those within the EU. In addition, there are requirements that Sweden has entered into an international security commitment with the country of the cloud service provider. The service provider need to be approved under the protective security legislation of such country, and commit to protective security obligations in a classified contract.

In light of the far-reaching requirements set out above, our assessment is that if the cloud service provider will process information classified as *confidential* or a higher classification, or have access to an operation of equivalent level of sensitivity, only Swedish cloud service providers who manage their own IT-infrastructure and do not provide access to classified information or security sensitive operations to its subcontractors should be considered.

4.3 The Financial Sector

4.3.1 OVERVIEW

A number of sector-specific regulations and security measures apply to banks and insurance companies and their outsourcing arrangements. First of all, it should be noted that banks and insurance companies may use cloud services, but they need to exercise caution and take a risk-based approach in regard to the terms and conditions to ensure that the agreements that they enter into do not contain limitations that complicate or hinder effective risk management, control, or supervision.

4.3.2 BANK SECRECY

Statutory bank secrecy does not prohibit banks from disclosing data about their customers. They are, however, prohibited from making *unauthorized* disclosures to a third party regarding any individual's relationship to banks. "Individual" here refers to both natural and legal persons. "Relationships to banks" refers to all information that the bank has access to or knows of regarding the customer concerning future, current and historical relations, regardless of the origin of such information.

Bank secrecy is statutory and is covered under the Swedish Banking and Financing Business Act (2004:297) ("**BFBA**"). On an EU level, the European Banking Agency ("**EBA**") mentions in its guidelines on out-

sourcing arrangements that upholding bank secrecy is one of the aspects that needs to be secured in outsourcing agreements.

It is not entirely clear how to interpret "disclosure" in regard to bank secrecy, specifically when an unauthorized disclosure should be deemed to have occurred. In essence, there are two possible interpretations of the term "disclosure":

- when a third party has *de facto* gained access to the data, for example by reading the information; or

- when a third party has been able to gain access to the data and thus has had the possibility to access the data (when there is no proof that they have actually accessed/read it).

In our opinion, the second interpretation is the most reasonable (and correct) interpretation under Swedish law. There are a number of indicative factors which point in this direction.

It should, however, be noted that an *authorized* disclosure is deemed to have occurred if the disclosure is necessary in order to protect the bank's business, for example in a dispute between a bank and its customer, or if a disclosure is made following the customer's consent. However, there is no valid consent if the customer only gives general consent, e.g. through signing the bank's terms and conditions – the consent must always be given in regard to a specific situation. There is no unauthorized disclosure if a bank engages a subcontractor and consequently discloses necessary data to the subcontractor in order to perform the agreement. Such disclosure is considered an authorized (lawful) disclosure. A situation where a bank is obligated to disclose data in accordance with Swedish or EU law is also considered an authorized disclosure.

Our assessment is that Swedish banks cannot make authorized disclosures of data in accordance with foreign law – such disclosures must be based on Swedish or EU law to be considered authorized. Banks should therefore be cautious and take a risk-based approach when engaging third country cloud providers which might be obligated to disclose data according to foreign law.

4.3.3 INSURANCE SECRECY

Insurance secrecy is not regulated by law, apart from the narrow exceptions in the Swedish Insurance Business Act (2010:2043) ("**SIBA**"). Insurance companies have, however, been voluntarily imposing secrecy and such secrecy has typically been regulated in customer agreements with policyholders. The scope and extent of insurance secrecy is comparable to those of bank secrecy. This should, in our opinion, entail that if a disclosure is considered as authorised according to the rules on bank secrecy, the same should apply to insurance secrecy as well, unless stated otherwise in law.

Our view is that insurance companies, just like banks, should be cautious when engaging third country cloud providers which might be obligated to disclose data according to foreign law, and should take on a risk-based approach. This assessment is based on the fact that insurance secrecy is extensive, the data can be sensitive (e.g. health declarations), and there are no guidelines (from e.g. Insurance Sweden) indicating otherwise. In addition, strict insurance secrecy should be considered as best practice in the industry.

4.3.4 REGULATORY REQUIREMENTS FOR OUTSOURCING BY BANKS AND INSURANCE COMPANIES (EBA AND EIOPA GUIDELINES)

The most predominant regulations for banks and insurance companies exist on EU level. Banks shall be compliant with EBA's guidelines on outsourcing arrangements, published in February 2019. Insurance companies shall be compliant with article 274 of the Solvency II delegated regulation[23] and the European Insurance and Occupational Pensions Authority's ("**EIOPA**") guidelines on outsourcing to cloud service providers. These regulations set out certain requirements on outsourcing arrangements, especially regarding critical and important functions, and the guidelines' requirements correspond to a large extent with each other, however not in every detail.

Both the EBA and EIOPA guidelines require banks and insurance companies to maintain control over their outsourced operations. Therefore, it is necessary that banks and insurance companies are able to make decisions and enforce them towards their cloud service providers, govern and manage their operations and ensure that they are able to insource and transition-back outsourced operations. The jurisdictional risk is therefore present in these situations as well.

Banks are also explicitly required to include an obligation for the cloud service provider to protect confidential, personal or otherwise sensitive data and to follow the same legal requirements regarding data protection that the banks are required to comply with. The regulatory requirements are therefore intertwined with the GDPR's requirements on data protection meaning, *inter alia*, that if a bank or an insurance undertaking commits a breach of the GDPR, it will also constitute a breach of the EBA and/or EIOPA guidelines. The same applies with regard to a breach of the bank secrecy and most likely a breach of the insurance secrecy as well, given that the EIOPA guidelines require insurance companies to apply an appropriate level of protection for confidential data.

23 Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

4.3.5 OUTSOURCING IN SECURITIES AND INVESTMENT SERVICES AND ACTIVITIES

When investment firms and banks carrying out investment services and activities, outsource to cloud providers, directive 2014/65/ EU on markets in financial instruments (MiFID II) and the delegated regulation (EU) 2017/565 for MiFID II apply instead of the EBA guidelines.

The European Securities and Markets Authority ("**ESMA**") published its final report on guidelines on outsourcing to cloud service providers in December 2020. The guidelines apply from the 31 July 2021 to all cloud outsourcing arrangements that are entered into, renewed or amended on or after that date. Any existing arrangement must be compliant with the guidelines no later than 31 December 2022.

Although MiFID II and ESMA's guidelines are similar to EBA's and EIOPA's guidelines, the ESMA guidelines provide a more detailed framework in regard to information security. This being said, ESMA's guidelines do not cover all aspects and risks relevant to the engagement of a cloud provider.

PART II

5. The Folke© Methodology

5.1 Overview

Kahn Pedersen has developed the Folke© Methodology as a way of visualizing the overall legal risks associated with public cloud services. The core elements of the methodology are "supplier risk" (cloud provider risk) and "information protection value", both of which are explained further in section 5.2 below.

We have developed the Folke© Methodology for the purpose of providing a dynamic and flexible decision-making tool for companies and organizations considering utilizing a public cloud service. To ensure this flexibility, the Folke© Methodology also considers the appropriate risk appetite of the specific cloud customer.

The Folke© Methodology is intended for situations where the result of the legal analysis and the legal assessment is not obvious, i.e. where there is no clear, 100% answer as to whether a particular cloud initiative is lawful or unlawful. By way of example, there is no real point in applying the Folke© Methodology to a case where, for example, an entity is considering processing information protected under the SPSA in a Chinese or US public cloud service (since the result is obvious from the outset).

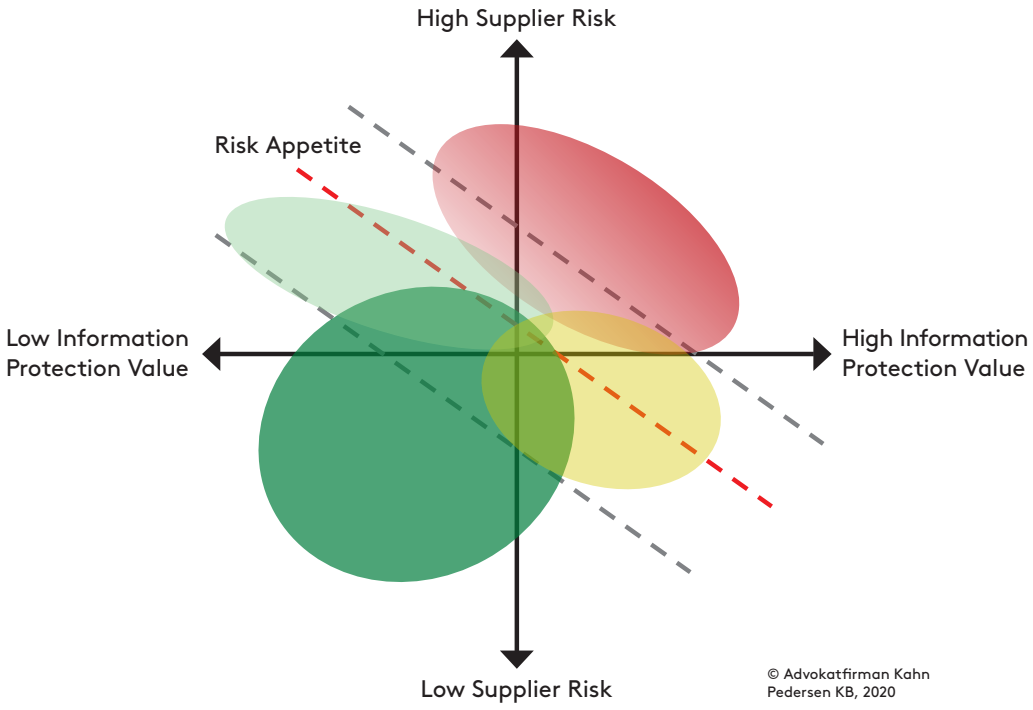


Figure 5.1: The Folke© Methodology.

5.2 Key Elements of the Folke© Methodology

5.2.1 SUPPLIER RISK

The ***y-axis*** of the Folke© Methodology is used to assess the level of supplier risk.

The level of supplier risk is typically rather fixed and difficult for an individual cloud customer to change or affect. Instead, the level of supplier risk is determined through a comprehensive legal and strategic assessment of: (i) the relevant cloud service; (ii) the relevant cloud provider; and (iii) the applicable contractual terms.

Cloud services and cloud service providers with a low level of supplier risk, e.g. a Swedish-owned and Swedish-operated private cloud service with robust and appropriate contract terms governed by Swedish law, should be placed on the lower part of the y-axis.

On the other hand, cloud services and cloud providers with a high supplier risk, e.g. a public cloud service provided by a supplier in a high-risk jurisdiction outside the EU/EEA, where the cloud service is regulated by one-sided, unbalanced, and/or seemingly arbitrary contract terms, would be placed on the upper part of the y-axis.

In particular, the following circumstances affect the supplier risk (please note that the list is not exhaustive).

- **Jurisdictional risk:** The extent of the jurisdictional risk is affected by, *inter alia*: (i) the wording of the confidentiality clause (and similar clauses) in the cloud contract; (ii) the governing law as per the cloud contract; (iii) other laws applicable to the supplier and/or potential subcontractors; and (iv) whether the data will be accessed from another location (e.g. through remote support services).

- **Geopolitical risk:** Is there a geopolitical risk (i.e. political instability, terrorism, sanctions, natural disasters, etc.) associated with the location where the data is stored?

- **Deviations in relation to other applicable jurisdictions:** Does compliance with regulations applicable to the cloud contract (and/or the cloud service) differ depending on the applicable jurisdiction?

- **Contractual terms and the cloud provider's control:** How robust are the contractual terms? For example, can the cloud provider unilaterally amend the contract and/or unilaterally suspend the service?

- **Availability:** How robust is the agreed level of availability of the cloud service (consider suspension rights, SLA-levels, etc.)?

- **Sanctions in the event of breach of contract:** Are breaches of the

terms of contract sufficiently sanctioned so as to have a deterrent effect on the cloud provider?

- **Operational dependency on the cloud service:** Is it practically possible for the cloud customer to take legal action against the cloud provider and/or to terminate the agreement prematurely, taking into account the cloud customer's dependency on the cloud service?

To summarize, when assessing the overall level of supplier risk, the following factors should be considered:

1. the choice of cloud provider;

2. the choice of cloud service and its structure/architecture; and

3. applicable cloud contract terms and conditions.

The following diagram illustrates how the choice of cloud provider, without negotiated contractual terms, will affect supplier risk and the corresponding positioning on the y-axis of the Folke© Methodology.

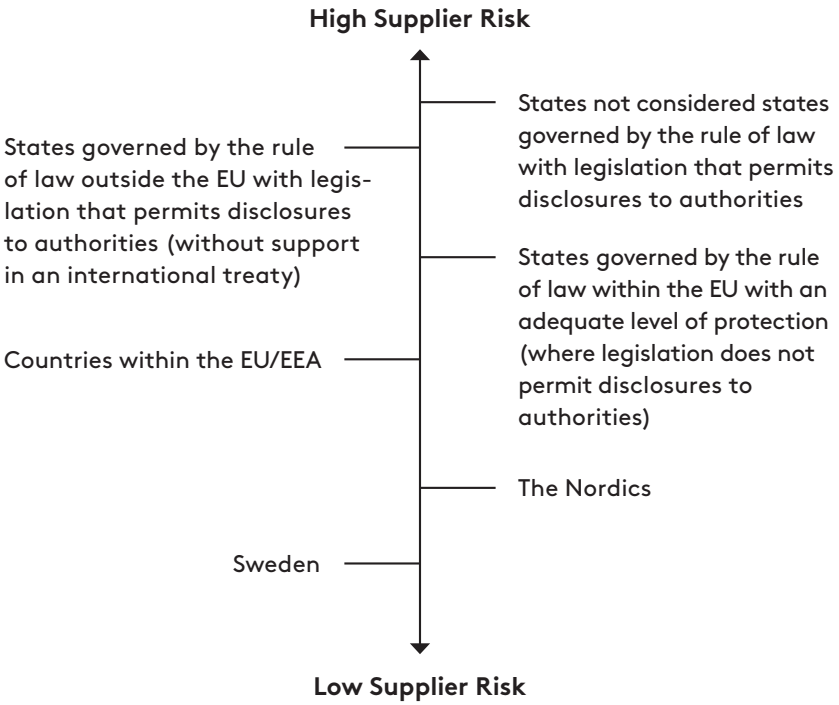


Figure 5.2: A closer look at the y-axis of the Folke© Methodology, focusing specifically on the choice of cloud provider and jurisdictional risk.

5.2.2 INFORMATION PROTECTION VALUE

The ***x-axis*** of the Folke© Methodology is used to assess the protection value of the data processed in the relevant cloud service.

Public cloud services can be used for many different purposes and for

many different types of data. Some types of information are more sensitive than other types as a consequence of, e.g., legal, security or commercial requirements and considerations. Therefore, a careful analysis and information classification is needed to assess which data is suitable to process in the cloud service.

Data with a low level of protection value is placed on the far left of the x-axis, while data with a high level of protection value is placed on the far right of the x-axis.

The information protection value is defined in the Folke© Methodology as the overall protection value that the data (standing alone and in the aggregate) has to the controller/owner of the data (i.e. the cloud customer), based on the legal, competitive, or commercial consequences of an unauthorized disclosure.

This risk is generally easier for the cloud customer to control than the supplier risk, since the cloud customer is in sole control in terms of determining which data will be migrated to the cloud.

The following circumstances, among others, affect the information protection value (please note that the list is not exhaustive).

- **Information classification:** Have the laws and regulations that apply in a particular case been identified (including any sector specific confidentiality requirements, e.g. in the banking or insurance sector or the health care sector)?

- **Sensitivity of the information:** What are the consequences of unauthorized disclosure? When considering this issue, the following factors need to be taken into account: (i) national security implications; (ii) implications for the stability of the financial/banking system in the cloud customer's jurisdiction; (iii) how critical the information is to the community where the customer is active; (iv) the privacy of the persons whose information is being processed (in cases where the information constitutes personal data); (v) the security interests covered by confidentiality provisions in applicable law; (vi) third-party interests (if the information is protected by confidentiality obligations towards a third party); (vii) the competitiveness of the cloud customer; and (viii) alternative ways of obtaining access to the information (e.g. other public sources).

- **Commercial value:** This must be assessed in terms of the data itself, in connection with metadata, and/or if aggregated together with other information. In particular, the cloud customer needs to assess whether the cloud provider considers the data to be valuable and whether the cloud contract entails that any data will in effect be "given away" to the supplier.

- **The Customer's continuity and exit plan:** The possibility and feasibility of moving the data and processing away from the cloud service provider at the end of the cloud contract.

To summarize, when assessing the level of information protection value, the following factors should be considered:

1. what data is processed in the cloud service;

2. which laws and regulations apply to such data;

3. how will the data be protected, and

4. how important and sensitive the information is for the cloud customer's business and other interests (such as national security, financial stability, the interests of co-operation partners, etc.).

The following diagram illustrates different categories of information and the positioning of such information on the x-axis of the Folke© Methodology.

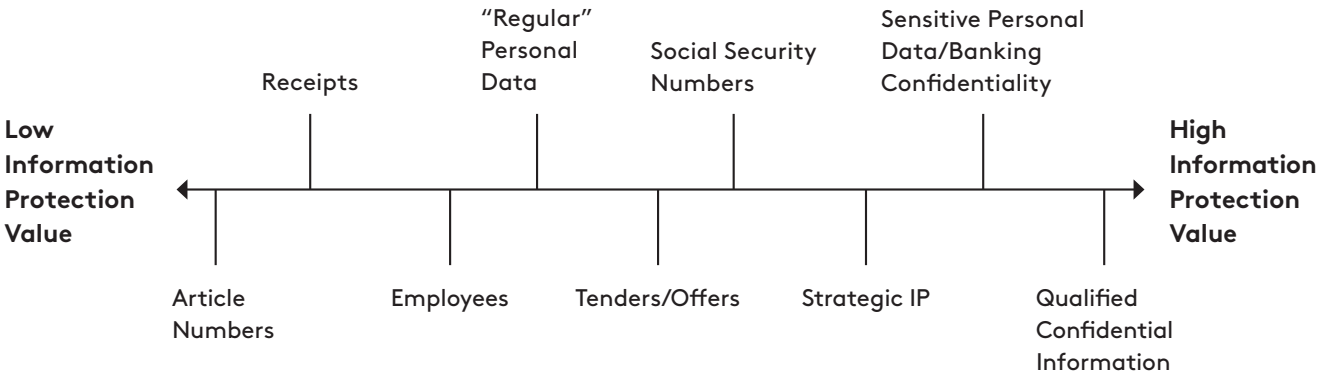


Figure 5.3: A closer look at the x-axis of the Folke© Methodology for different pieces of information.

5.3 Combining Supplier Risk with Information Protection Value

As described above, the Folke© Methodology is used to assess "supplier risk" and "information protection value". When these two aspects are combined and mapped onto the x-axis and y-axis of the Folke© Methodology, the result will be placed in one of four different areas:

- Dark green area = low supplier risk and low information protection value

- Light green area = medium/high supplier risk and low information protection value

- Yellow area = low/medium supplier risk and high information protection value

- Red area = high supplier risk and high information protection value

Use of cloud services that is placed in the red area is typically associated with high legal risks. The light green and light yellow areas of the Folke© Methodology represent a medium-low and medium-high level of collective risk, respectively. The dark green area will, of course, signal a low legal risk associated with the relevant cloud service.

It should be emphasized that the Folke© Methodology is dynamic, insofar as the result will be affected depending on the legal, contractual, technical, and organizational protection measures taken. By taking various measures the cloud customer can influence and mitigate the risks involved. For instance, by negotiating the terms of the cloud contract, a cloud customer can reduce the supplier risk on the y-axis. Similarly, excluding certain types of data and/or introducing additional technical security measures may reduce the information protection value on the x-axis.

5.4 Adding Risk Appetite

As mentioned above, the Folke© Methodology also takes into consideration the risk appetite of each potential cloud customer, as determined by the cloud customer itself. In assessing the level of risk appetite, the cloud customer should take as its starting point the laws and regulations that apply to the relevant business/industry in question and to the information being processed. In addition, the cloud customer should also take into account market-specific and commercial factors. The risk appetite should also be influenced by the advantages (e.g. reduced costs, shortened time-to-market, or increased flexibility) that the cloud service will afford the cloud customer when compared to alternative (on-premises) solutions.

The risk appetite of the cloud customer is illustrated by the broken red diagonal line in the model and should, typically, be placed somewhere between the two broken grey diagonal lines. Assessments that result in a risk placement above the broken red line should generally be considered unacceptable and/or impermissible by the cloud customer, while placements under the broken red line should generally be considered acceptable by the cloud customer.

5.5 Mapping Common Public Cloud Services in the Folke© Methodology

The following overview illustrates how the most common cloud services and information types may be plotted on the different axes of the Folke© Methodology.

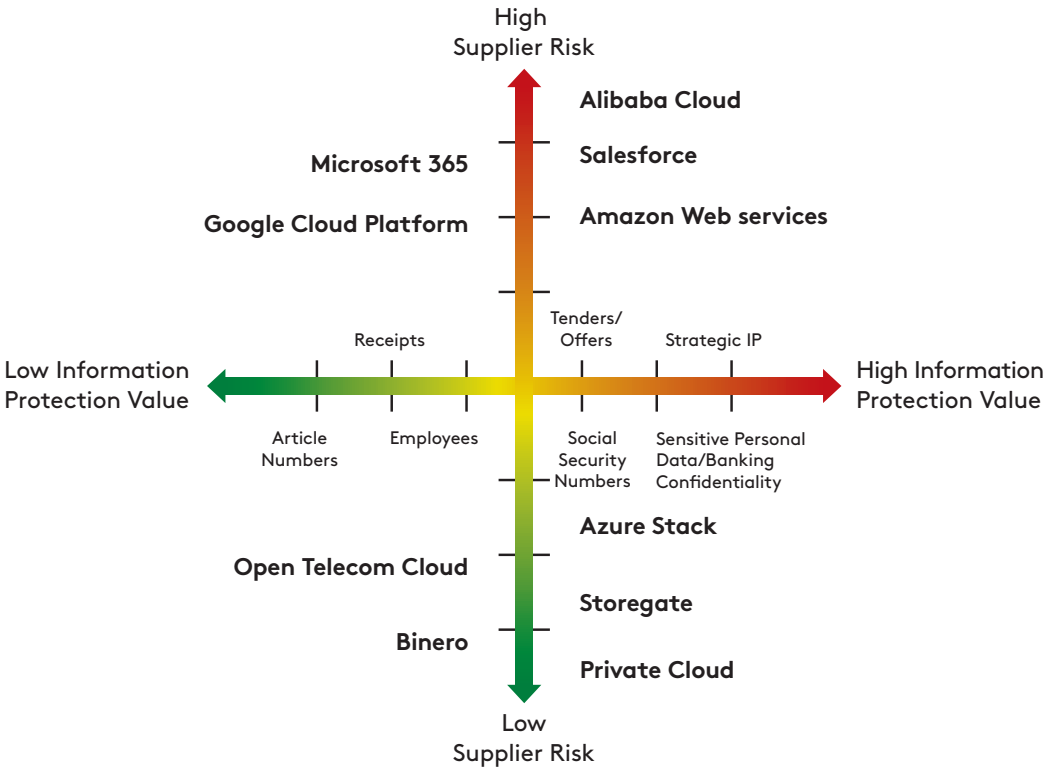


Figure 5.4: A few of the most common cloud services together with different information types, inserted in the Folke© Methodology.

Please note that the examples presented in this section by no means represent a complete analysis of the possible scenarios in which the Folke© Methodology may be applied.

As is clearly shown in the diagram above, application of our assessment entails that the major US cloud providers and their (non-negotiated) standard cloud contracts should typically, in our opinion, be placed on the upper part of the y-axis. The reasons for this opinion are that, firstly, the standard contract terms are typically one-sided, unreasonable, and inadequate and, secondly, there is a significant level of jurisdictional risk created by the conflict of laws between the EU and the US.

However, this assessment does not mean that the use of cloud services offered by US cloud providers should always be considered impermissible or unlawful. On the contrary, what this illustrates is that use of such cloud services is dependent on meticulous planning and implementation of extensive measures in order to effectively mitigate and reduce the initial level of supplier risk.

6. Use Cases for the Folke© Methodology

In this chapter, we will use the Folke© Methodology in two fictional scenarios where US-based cloud services are being considered.

6.1 Scenario 1: An Industrial-Engineering Company Considering a Resource Planning Tool (SaaS)

An industrial company based in Sweden is considering entering into an agreement with an American cloud provider regarding a SaaS for resource planning. The information that would be processed within the cloud service mainly relates to the business' accounting, ongoing projects, financial management and procurement (all of which may contain information that constitutes personal data and information that is commercially sensitive for the company). In this example, the company is the data controller and the cloud provider will take on the role of data processor for the company. The information will be stored in the cloud provider's data center within the EU/EEA. The company decides that it has a medium risk appetite.

A. Situation 1: Starting point

SUPPLIER RISK: Medium/High, based on the following factors:	
1. The cloud provider	• A cloud provider which is US-based and subject to US law, risk of disclosure of information to authorities
2. The cloud service	• SaaS that will result in unencrypted processing of information • Data stored on servers within the EU/EEA
3. Terms of the agreement	• All the usual risks associated with cloud service agreements are expected to apply • The cloud provider's standard agreement is estimated to be more balanced than many other standard agreements for cloud services • The cloud provider's standard agreement is governed by Swedish law • The cloud provider's data processing agreement meets the majority of the requirements in the GDPR

THE INFORMATION PROTECTION VALUE: Medium, based on the following factors:	
1. The information	• The main types of information are data about the company's finances, projects, employees, and transactions • The processing includes personal data (possibly also social security numbers) • Commercially sensitive information (i.e. trade secrets) will be processed • No data that is covered by the SPSA • No processing of sensitive personal data • No data that includes details on criminal activity, children, or other particularly vulnerable subjects • No data that is covered by the Swedish Public Access to Information and Secrecy Act (2009:400)
2. Laws applicable to the information	• GDPR with accompanying frameworks • The Swedish Act on the Protection of Trade Secrets (2018:558)
3. Security measures	• The technical security level is estimated to be in line with what one might expect from a public cloud service (e.g. encryption, high physical security, etc.) • Certain specific security and follow-up possibilities for the company are missing
4. The importance of the information for the company	• A disclosure of the information to a foreign authority is estimated to cause the company considerable commercial harm

THE CUSTOMER'S RISK APPETITE: Medium/High, based on the following factors:	
1. Laws and regulations applicable to the company and the information	• The Swedish Act on the Protection of Trade Secrets (2018:558) • GDPR with accompanying frameworks
2. Market-specific and commercial factors	• Competitors on the company's market are estimated to gain a competitive advantage if they use cloud services • A disclosure of the information to a foreign authority is estimated to cause the company considerable commercial harm
3. Assumed benefits in relation to alternative solutions	• Reduced costs • Increased flexibility • Immediate access to new versions and security patches for the software • Access to a higher level of competence within IT infrastructure • A generally higher level of technical security measures

The company determines that the combined risk of using the service without taking further measures is placed in the red area in the Folke© Methodology, which exceeds the company's risk appetite. The company should therefore not accept such use.

In order to adjust the risk to such an extent that it would be possible for the company to use a cloud service for the purpose in question, the company implements the following risk mitigation measures:

- taking inventory of the personal data in the information to be processed through the cloud service;
- excluding sensitive personal data from the processing;
- ensuring that the company's information is separated from other customers' information in the cloud environment,
- encrypting the company's information using strong encryption methods in transit and at rest; and
- ensuring that the data at rest is stored within the EU/EAA.

B. Situation 2: Proposed changes

The initial risk measures taken by the company place the combined risk associated with the use of the cloud service in the light green area in the Folke© Methodology, which signifies a medium-low supplier risk.

If, in addition to the initial risk measures, the company also chooses to take the additional measures outlined below, the weighted risk will be adjusted so that it is placed in the dark green area of the Folke© Methodology. Such use falls within the company's general risk appetite. Further measures that the company may take to reduce the risk are:

1. Negotiation of the terms of the contract	• Adding explicit and clear obligations as regards decisive IT security measures • Including an obligation that the cloud provider does not relocate the company's data to another data center within the EU/EEA without the company's prior consent • Introducing an audit right for the company regarding the cloud provider's IT security measures
2. Data security related measures	• Ensuring that the company is not data processor for e.g. its customers as regards any personal data that will be covered by the service • Reviewing and updating informational texts to data subjects • Documenting the company's introductory data processing analysis (i.e. no need for a data protection impact assessment) • Establishing and implementing adequate processes for data minimization and purpose limitation

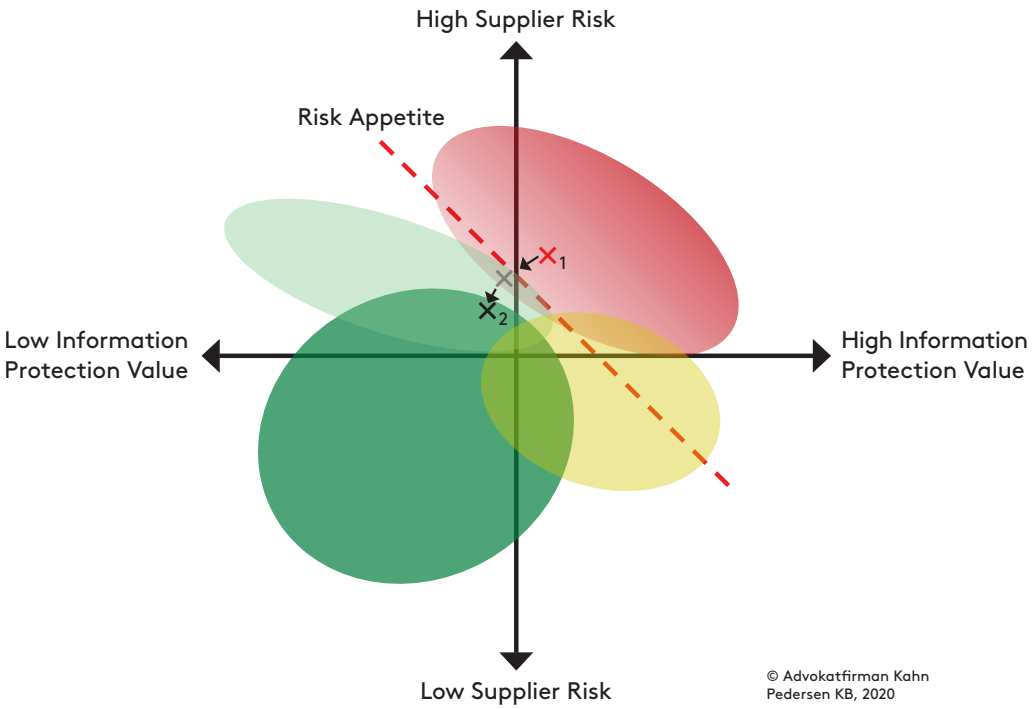


Figure 5.5: The industrial company's risk assessment of the planned use of the SaaS, illustrated using the Folke© Methodology.

6.2 Scenario 2: A Bank Considering Web-based Office Tools (SaaS)

A Swedish bank is considering entering into an agreement with a US cloud provider regarding the use of a SaaS for office services. The information that the bank would handle within the framework of the cloud service may contain both information that constitutes personal data and information about the bank's customers (which is covered by the rules on bank secrecy in the Swedish Banking and Financing Business Act (2004:297) and the EBA's guidelines for outsourcing). In this example, the bank is the data controller and the cloud provider will take on the role of data processor. The information will be stored in the cloud provider's data center within the EU/EEA. The bank decides that it has a low/medium risk appetite.

A. Situation 1: Starting point

SUPPLIER RISK: High, based on the following factors:	
1. The cloud provider	• A cloud provider which is US based and subject to US law, risk of disclosure of information to authorities
2. The cloud service	• SaaS that will result in unencrypted processing of information • Data stored on servers within the EU/EEA
3. Terms of the agreement	• All the usual risks associated with cloud service agreements are expected to apply • The cloud provider's standard agreement is estimated to be more unbalanced than many other standard agreements for cloud services • The cloud provider's standard agreement is not governed by Swedish law • The cloud provider's data processing agreement does not meet the requirements in the GDPR to the same extent as data processing agreements of other cloud providers

THE INFORMATION PROTECTION VALUE: High, based on the following factors:	
1. The information	• The bank has not limited the type of information which may be processed in the service • The processing includes personal data (including social security numbers) • The processing includes information about the bank's customers • The processing may include sensitive personal data • Commercially sensitive information (i.e. trade secrets) may be processed • There is no data that is covered by the SPSA • The processing applies to a large number of data subjects
2. Laws applicable to the information	• GDPR with accompanying frameworks • The Swedish Banking and Financing Business Act (2004:297) • The Swedish Act on the Protection of Trade Secrets (2018:558)
3. Security measures	• The technical security level is estimated to be in line with what one might expect from a public cloud service (e.g. encryption, high physical security, etc.) • Certain specific security and follow-up possibilities for the company are missing
4. The importance of the information for the company	• An unauthorized disclosure may have serious consequences for the data subjects' privacy and may lead to sanctions from regulatory authorities and, ultimately, a revocation of the bank's license • A disclosure of the information to a foreign authority is estimated to cause the company considerable commercial harm

THE CUSTOMER'S RISK APPETITE: Low/Medium, based on the following factors:	
1. Laws and regulations applicable to the company and the information	• The Swedish Banking and Financing Business Act (2004:297) • EBA's guidelines for outsourcing • The Swedish Act on the Protection of Trade Secrets (2018:558) • GDPR with accompanying frameworks
2. Market-specific and commercial factors	• Regulated market • Highly competitive market • Dependency on substantial customer confidence • An unauthorized disclosure may lead to sanctions from regulatory authorities and, ultimately, a revocation of the bank's license • A disclosure of the information to a foreign authority is estimated to cause the company considerable commercial harm
3. Assumed benefits in relation to alternative solutions	• Reduced costs • More versatile handling of customer and employee matters • Increased flexibility

The bank has not taken any specific technical security measures and makes the assessment that the combined risk of the planned use of the cloud service without such measures is placed in the red area in the Folke© Methodology, which exceeds the bank's risk appetite. The bank should therefore not use the cloud service.

B. Situation 2: Proposed changes

The unlimited processing of the information that the bank plans to implement would include information about the bank's customers, which would, *inter alia*, be in breach of the rules on bank secrecy in the Swedish Banking and Financing Business Act (2004:297). In order for the bank to be able to use the cloud service, the bank needs to limit the use of the service in such a way that the information processed does not include information about the bank's customers. The bank chooses to take the additional measures outlined below, which, according to the bank's assessment, will result in the weighted risk being adjusted and placed in the dark green area of the Folke© Methodology. Such use falls within the bank's general risk appetite.

1. Limitations regarding the bank's use of the service	• Elimination of customer data from the data processed in the cloud service, establishing alternative communication channels for communication with customers (which are not cloud services) • Minimizing the processing of personal data in the cloud service by storing sensitive personal data in a separate system (which is not a cloud service)
2. Negotiation of the terms of the contract	• Adding explicit and clear obligations as regards decisive IT security measures • Including an obligation that the cloud provider does not relocate the company's data to another data center within the EU/EEA without the company's prior consent • Introducing an audit right for the company regarding the cloud provider's IT security measures • Ensuring that the cloud provider's data processing agreement meets the requirements in the GDPR
3. Data security related measures	• Reviewing and updating informational texts to data subjects • Documenting the company's introductory data processing analysis and data protection impact assessment • Establishing and implementing adequate processes for data minimization and purpose limitation
4. Technical and organizational security measures	• Ensuring strong encryption of the bank's information • Joining the cloud provider's "compliance program" • Strengthening the bank's continuity protection and exit planning

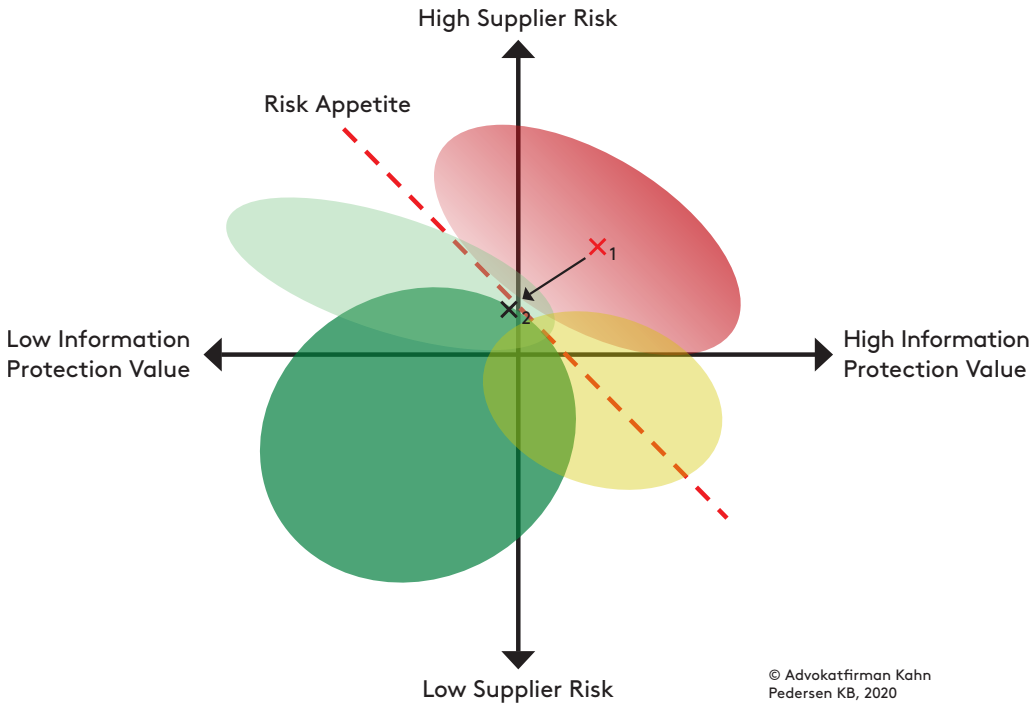


Figure 5.6: The bank's risk assessment of the planned use of the SaaS, illustrated using the Folke© Methodology.

www.kahnpedersen.se