EuroCloud AUSTRIA

GUIDELINE

CLOUD COMPUTING

CLOUD & DATA PROTECTION

THE CLOUD PRIVACY CHECK (CPC)

AUSTRIA
GERMANY
SWITZERLAND



Imprint

EuroCloud Austria
Verein zur Förderung von Cloud Computing
Museumstraße 5/14
1070 Wien

E-mail: info@eurocloud.at
Web: http://www.eurocloud.at

Copyright: EuroCloud Austria Verein zur Förderung von Cloud Computing. 2015

Table of Contents

1. Introduction 6

1.1 Where Things Become Serious 6
1.2 We Are Making Things Difficult for Ourselves 6
1.3 The Methodology of the CPC 7

2. Data Protection and Cloud Computing 8

2.1 General Information on Data Protection 8
2.2 Data Protection Considerations in Regard to Cloud Services 8
2.3 Two Central Rules of Data Protection Law 10

3. Cloud Privacy Check (CPC) 10

3.1 The CPC Solves a Perception Problem 10
3.2 Terminology of the CPC 11
3.3 What Does the CPC Address? What Doesn't It Address? 12
3.4 Basic Criteria of the CPC 12
3.5 The Four Steps of the CPC 14

4. Legal Explanations on the Individual Steps of the CPC 14

4.1 The Toolbox 14
4.2 The Four-Step Model 16

5. Particularities of National Data Protection Laws 20

5.1 Application of National Data Protection Law 20
5.2 Austria – Particularities in Data Protection for Cloud Computing 21
5.3 Germany – Particularities in Data Protection for Cloud Computing 23
5.4 Switzerland – Particularities in Data Protection for Cloud Computing 25

6. Prospect: Draft of an EU-GDPR (EU-GDPR-D) 27

7. Conclusion 28

8. Cloud Computing Glossary 29

9 Legal Information 30

10. Authors 31

Foreword



Dr. Tobias Höllwarth
Director, EuroCloud Austria

Until recently, it seemed almost to be good form to ignore or even completely block out the topic of cloud computing. This early phase of development of one particular part of the digital revolution we are currently witnessing can now be considered over, however. Today, nobody would contend that cloud computing will be anything but a significant aspect of IT sourcing in the years to come.

This also makes immediately clear that comprehensive knowledge in many areas – not just in technology – is required if one intends to utilise cloud services seriously, responsibly, profitably, and in a manner compliant with the locally relevant legal frameworks.

The topic of data protection is one of the first to come to mind, since the use of cloud services implies that data – including personal data – are transmitted to others for processing. Unfortunately, here in Europe it is not only our many different languages that make things difficult for us: Cloud service providers and users are faced with major obstacles in regard to data protection, causing us to suffer massive and unacceptable competitive disadvantages in comparison with, for example, the USA.

This prohibitive state of affairs must be remedied as quickly as possible at the EU and member state levels. Unfortunately, it will likely take a while for things to change – but until then, this guideline outlining the Cloud Privacy Check (CPC) is intended to simplify certain decisions and processes for most affected persons. Naturally, it cannot replace legal expertise, but it structures and breaks down a complex topic without withholding any vital information.

This guideline was created in the framework of the Trust-in-Cloud project and is the result of several months of development by the CPC team, to whom I wish to express my thanks: Dr. Clemens Thiele (Austria), Dr. Jens Eckhardt (Germany), and Dr. Christian Laux (Switzerland).

Vienna, November 2015

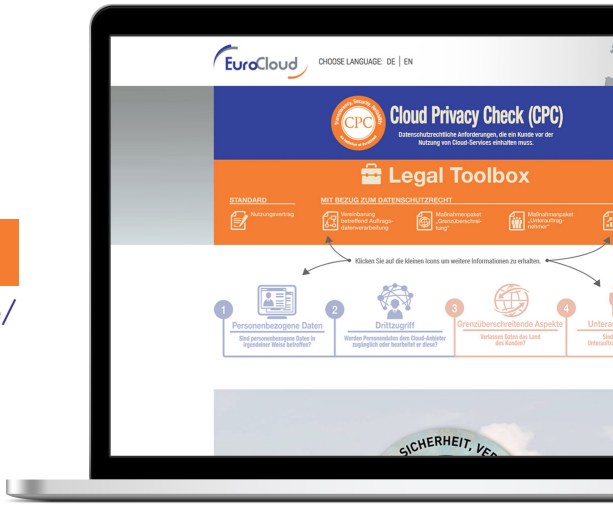
Dr. Tobias Höllwarth

Director, EuroCloud Austria

Transparency, Security, Reliability
CPC
An Initiative of EuroCloud

CPC ONLINE TOOL

http://www.cloudprivacycheck.eu/de/



1 Introduction

1.1 Where Things Become Serious

Anyone who transmits personal data into a cloud service for the first time knows that this is a critical moment.

It is critical because it makes one intensely aware of one's dependence on an externally procured service and its provider. It is critical because the integration of a cloud service into an existing corporate IT structure is a complex outsourcing project that can potentially reveal one's own weaknesses, lack of knowledge, and incompatibilities ¬– as well as those of the provider. Last but not least, it is also critical because the transmission of personal data to a third party (a contractor), sometimes even to another country, is a process that is usually subject to strict legal conditions and regulations. In other words: Any grave mistake made here can result in serious commercial and legal consequences as well as damaged reputations.

Cloud sourcing is a complex outsourcing process heavily influenced by legal requirements. In Europe, providers and users of cloud services face more than mere language obstacles. The particularities in each of the different EU member states in regard to data protection play a large role in making the buying and selling of cloud services across national borders an arduous process. The effort required can be economically quantified, for the costs of initiating such transactions – as well as the costs of purchasing and evaluating services – can be measured.

1.2 We Are Making Things Difficult for Ourselves

Understanding the complexity of current European data protection laws and regulations is already difficult enough for an IT engineer, buyer, or business user. In combination with the often small but nevertheless significant differences between various EU member states, however, it can become an almost insurmountable challenge without proper juristic accompaniment from the very start.

Upshot: Here in the EU we are making things more difficult for ourselves than necessary. There is a general consensus that this competitive disadvantage needs to be remedied quickly, and this will be achieved to some degree by the European Data Protection Directive. We should immediately do away with all too optimistic illusions, however. Full applicability of the directive itself, and even more so the removal of country-specific regulations from it, will certainly require lengthy transition periods to achieve.

1.3 The Methodology of the CPC

This means there is need for immediate relief. This guideline and the Cloud Privacy Check (CPC) are intended to provide that relief by employing three methodical approaches:

The Cloud Privacy Check (CPC) employs three methodical approaches: Simplification, Structuring, and Separation.

1. Simplification

Simplification of a complex subject matter without loss in terms of content. The goal of the CPC is to elucidate the topic of data protection in the cloud to 90 percent on a single page, thus providing a comprehensible and workable basis of information for 90 percent of the people having to deal with the topic. But don't worry: jurists will still be needed.

2. Structuring

Structuring of a plethora of questions into individual topical blocks which can then be approached step by step – from the simplest to the most complex case. Simultaneous correlation of the respectively required legal tools to be generated and evaluated in detail by jurists.

3. Separation

Separation of the generally applicable from the specific. This is probably the most significant aid for managing a complex trans-border endeavour. By identifying what is the same throughout all countries, the CPC allows the user to focus on the differences – if they actually apply to him. The CPC aims to provide access to relevant information affecting another country quickly and easily, without having to deal with those aspects that are the same as "at home".

This guideline follows similar principles to those of the CPC itself. It begins with a basic and easily understandable introduction to the topic before explaining the application of the CPC. A description of the legal tools which may need to be applied is included as well as, ultimately, the presentation of country-specific features and peculiarities – limited, in this particular guideline booklet, to the DACH region (Germany, Austria, and Switzerland).

2 Data Protection and Cloud Computing

2.1 General Information on Data Protection

Data protection law is a general term for the standards of a legal system concerning the protection of personal data. The protection of personal data serves the purpose of protecting the privacy of the affected person, and the fundamental right of humans to privacy must be protected also in the information society. The central framework of data protection law in the member states of the EU and the European Economic Area is the Data Protection Directive.[1]

The protection of personal data serves to protect persons, not to protect data as an end in itself.

The protection of personal data serves the protection of persons. Hence it is not the data themselves which are to be protected as an end in itself.

In order to **protect the privacy of persons**, data protection law primarily grants a right to **confidentiality of personal data**, so long as there exists a legitimate interest to do so.[2] This right can be curtailed in particular with the consent of the affected person or to protect the overriding legitimate interests of others. There also exist additional entitlements of the affected person (namely the right to access, correction and deletion).

Data protection law is characterized by the principle of rules and exceptions. Anyone processing the personal data of others requires a justification to do so.

The regulations of data protection law apply irrespective of contractual regulations. Data protection regulations apply to any type of data processing, whether online or offline.[3]

Data protection law is characterized by the principle of rules and exceptions. Anyone processing the personal data of others requires a justification to do so.

2.2 Data Protection Considerations in Regard to Cloud Services

"Cloud" is the collective term for server-based offerings for data processing.

Cloud services provide a high potential for increasing efficiency in the business world. However, from a data protection perspective, the following aspects are identified as critical:

1 RL 95/46/EG. Member state are required to incorporate the Data Protection Directive into national law. In the future, the Data Protection Directive (and with it the national execution laws) is to be replaced by a uniform basic Data Protection Regulation.

2 Article 1(a) RL 95/46/EC.

3 The European Court of Justice (ECJ) has established this fact in the year 2003 in the Lindqvist case (ECJ 6.11.2003, C-101/01).

Risk due to involvement of a third party: With the Cloud Service Provider (CSP), a third party becomes involved in the processing of personal data by the Cloud Service Customer (CSC). From the point of view of the affected person whose rights are to be protected, this represents an increase in the risk that unauthorized persons might be able to access the data being processed.

Loss of control: An increase in the number of people authorized to access the processed data means an increase in the challenge of committing all involved persons to act according to data protection laws, as well as the challenge of verifying the observance of all data protection obligations. The term "loss of control" refers to the fact that the affected person often does not know who the authorized third parties are, or has no way of monitoring them.

The use of cloud services seems to be accompanied by serious obstacles for the cloud user in terms of data protection.

These concerns can be put into perspective as follows, however:

The use of cloud services seems to be accompanied by serious obstacles for the cloud user in terms of data protection.

On risks due to the involvement of a third party: These risks are not actually new. Already before the introduction of cloud services, the division of labour in the digital world had been characterized by the involvement of third parties for the processing of personal data. In fact, data protection law already offers a suitable tool for managing this situation in the form of so-called "contracted data processing". Properly devised cloud services are actually capable of providing better protection against unauthorized accessing of personal data than traditional outsourcing infrastructures.

On the fear of loss of control: This concern may have been fuelled by the image of the "cloud". While it is true that the provision of cloud services often occurs with the involvement of third parties as well as across national borders, this is nothing new to data protection laws and has already been standard practice for a long time. The peculiarity of cloud services may be the fact that such constellations are now coming into widespread and mass-market use. This does not change anything the fact that these constellations are perfectly controllable from the legal perspective of data protection. For the involvement of subcontractors, data protection law offers the tool of contracted data processing, and the individual data protection laws stipulate specific requirements for trans-border data processing.

Data protection law is capable of regulating cloud services in compliance with the requirements of data protection

In summary, there is no doubt that data protection law is capable of regulating cloud services in compliance with the requirements of data protection. The reason for concerns regarding cloud services is apparently twofold: (1) various data-protection-related requirements apply to cloud services; (2) the circumstances affecting them are complex.

2.3 Two Central Rules of Data Protection Law

Data protection law stipulates two central rules which are particularly significant for cloud services:

Responsibility of the Cloud Service Customer (CSC):

With the use of cloud services, the CSC remains responsible for compliance with data protection law within the framework of the employed cloud services. No delegation of this responsibility to the Cloud Service Provider (CSP) takes place. In simple terms, the same basic principles apply the same way as they would if the CSC were to process the data on its own systems without involving a CSP.

Cloud Service Provider (CSP) as contracted data processor:

The Cloud Service Provider (CSP) operates as a so-called contracted data processor as defined by data protection law. This status as contracted data processor is the preferable involvement of the CSP in terms of data protection law. The CSP remains a legally separate entity which, however, processes personal data on behalf of the CSC, who remains the party responsible for the processing.

3 Cloud Privacy Check (CPC)

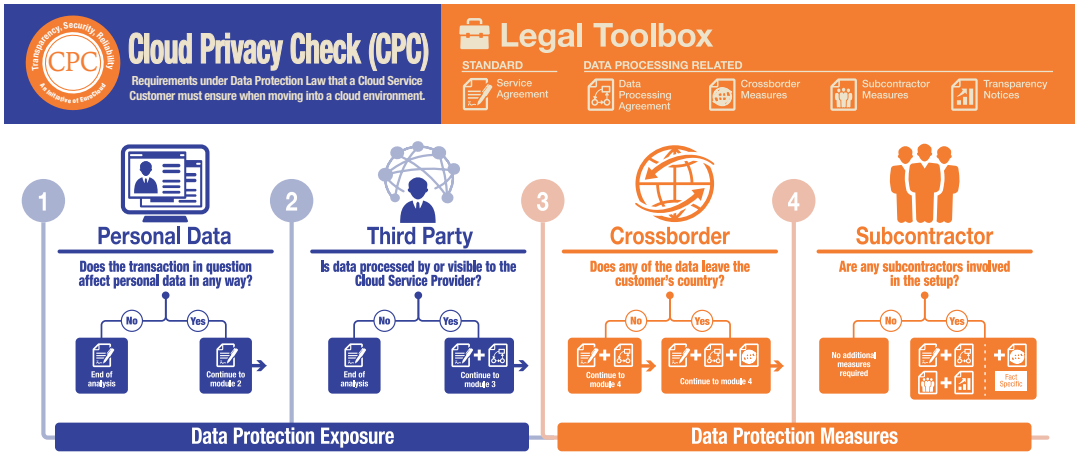
3.1 The CPC Solves a Perception Problem

Experience has shown that legal analysis in terms of data protection is overly complex in parts, which promotes legal uncertainty rather than reducing it.

The Cloud Privacy Check (CPC) counteracts this complexity:

SYSTEMATICS: First and foremost, the CPC establishes that the fundamental questions can be approached systematically as they are addressed in the data protection laws of various legislations. The CPC clearly illustrates these fundamental questions.

TOOLBOX: Furthermore, the CPC also shows that the abovementioned fundamental questions can be answered using the appropriate instruments (CPC Toolbox) provided by data protection law.



The Cloud Privacy Check clarifies the fundamental questions and points out the relevant instruments provided by data protection law.

3.2 Terminology of the CPC

A frequent problem for the classification of cloud services in terms of data protection law is inconsistent terminology. Because data protection law did not anticipate cloud computing, the relevant data protection terminology has not yet been properly "translated" for cloud computing.

In order to alleviate this terminological confusion, the CPC unambiguously defines the terminology of the cloud industry as follows:

Cloud Service Customer (CSC): The customer of a cloud service is referred to as the Cloud Service Customer (CSC). The CSC is at the centre of our economic considerations for this guideline.

Cloud Service Provider (CSP): The CSP is the service provider supplying the cloud service to the CSC.

Cloud Data Subject (CDS): The affected person, referred to as the CDS, is the focus of our data protection considerations. The CSC transfers data of the CDS into the cloud, and this is the reason for all of the issues relating to data protection (increase of risk and loss of control).[4] Despite this transfer of data into the cloud, the CDS must be protected by data protection law.

4 See above, Section II.B

Personal data: Data are relevant in terms of data protection law only if they contain some reference to the CDS. Only then are they referred to as personal data. The reference to the CDS must be clear enough that the affected person can be identified. Identifiability is the case if further information can be procured without disproportionate effort which allows the person to be positively identified. Hence it is sufficient if the CSP can determine who the affected person (CDS) is by way of further enquiry for the rules of data protection law to become applicable.[5]

3.3 What Does the CPC Address? What Doesn't It Address?

The CSC may only process data of the CDS lawfully, inside or outside of the cloud. Any applicable processing restriction must already be complied with by the CSC, and they must be passed on from the CSC to the CSP. The CPC does not deal with this aspect of data protection that applies regardless of the utilisation of cloud services.

The CSC must likewise comply with the two aforementioned central rules of data protection law.[6] In regard to the CDS, the CSC must ensure its protection as required by data protection law with a view to the particularity of the use of cloud services. These are the cloud-specific questions of data protection, and the CPC addresses these questions.

3.4 Basic Criteria of the CPC

Criterion #1: Personal data: The CPC applies whenever personal data of a CDS are processed.

Criterion #2: Involvement of a third party: The CPC takes account of the fact that cloud services may be supplied by external providers.

Criterion #3: Trans-border relevance: External service providers often supply their services in or from foreign countries.

Criterion #4: Subcontractors: External service providers also frequently employ further subcontracted service providers in order to supply the cloud service. These subcontracted service providers may in turn supply their part of the service in or from further countries.

5 *See also the information in Section IV.B*

6 *See above, Section II.C.*

This means that within the framework of any data protection law within the EU and the EEA, as well as those of Switzerland and Turkey, four fundamental questions arise in the evaluation of cloud services in terms of data protection

Within the framework of any data protection law within the EU and the EEA, as well as those of Switzerland and Turkey, four fundamental questions arise in the evaluation of cloud services in terms of data protection.

Practical example: It is not unusual for a domestic CSP to have the data centre service required for the CSP's cloud service supplied by a foreign company. Software maintenance and/or software development, as well as support, may be handled by further foreign companies (keywords: "offshoring" and "follow the sun"). Note: Although the CSP is a domestic company, the circumstances create trans-border relevance.

Practical example: If the CSP is a foreign company and the remainder of the supply chain is as described in the previous example, the trans-border relevance is apparent.

Each of the four mentioned fundamental questions (see above: Criteria #1 to #4) represents a crossroads in terms of data protection law. Depending on the answers to these questions, data protection law imposes certain measures to ensure data protection.

The CPC processes these four fundamental questions in four steps and provides appropriate answers. By doing so, the CPC illustrates the following:

The evaluation of cloud services can be broken down into four fundamental questions. Cloud services can be used in compliance with data protection law if these four fundamental questions are answered appropriately and the corresponding required measures are taken.

The evaluation of cloud services can be broken down into four fundamental questions, allowing a comprehensive evaluation of cloud services in four steps.

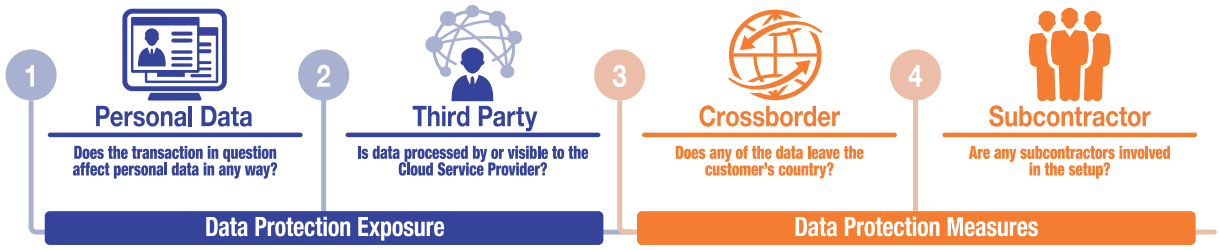
Cloud services can be used in compliance with data protection law if the four fundamental questions are answered appropriately and the corresponding required measures are taken.

3.5 The Four Steps of the CPC

Criterion #1 (personal data) and Criterion #2 (third party involvement) together address the question whether the use of the cloud service is relevant in regard to data protection law. Taken together, these two criteria mark the transition point in the analysis relating to data protection law. The CPC considers these two criteria in steps 1 and 2.

Steps 3 and 4 of the CPC address the data protection measures for certain constellations typical for cloud services.

The total result is the four-step process that is the CPC. Its individual steps are described in detail in Section IV.B.



4 Legal Explanations on the Individual Steps of the CPC

Each of the four steps of the CPC deals with data-protection-relevant questions and aspects of the configuration of the use of cloud services.

4.1 The Toolbox

The individual packages of measures introduced below are described in more detail in the context of the respective steps of the CPC as well as in Section V.



From the perspective of data protection law, a cloud service is being lawfully employed if the correct instruments are being used for it.

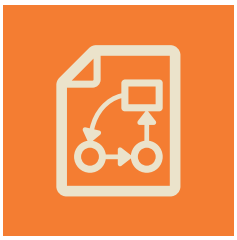
1. Cloud Service Agreement



A service agreement in regard to the cloud service is required. In the service agreement, the service obligations of the CSC and the CSP are defined in terms of civil law. The core of the defined obligation of the CSC is payment of the service fees. The core of the defined obligation of the CSP is the provision of the cloud service. Whether further provisions are included – and what they are – depends on the requirements of the contract parties (e.g. provisions regarding late payment, blocking of the service, the service level, availability, performance, etc.).

Besides the generally required cloud service agreement, the so-called "CPC Legal Toolbox" contains four further instruments:

2. Data Processing Agreement



The data processing agreement is a contract for whose content the governing national law specifies certain requirements.[7] If these requirements are met, the contract defines the privileged involvement of a contractor in accordance with data protection law.

Therefore, it is a preferable form for the involvement of contractors.

3. Cross-border Measures



The "cross-border" package of measures includes guidelines for data-protection-compliant configuration of cross-border data processing. There are various differences to observe depending on which country the data are transferred to.[8]

7 See the presentation of particularities of national legal systems (Section V).

8 National particularities are presented in Section V.



4. Subcontractor Measures

The "subcontractor" package of measures includes guidelines for the involvement of subcontractors by the CSP. Special requirements apply to this constellation due to the data processing agreement (see Section IV.A.2) as well as due to possible further cross-border data processing (see Section IV.A.3).[9]



5. Notice to Customer for Increased Transparency

Particularly the involvement of subcontractors creates a transparency obligation for the CSP vis-à-vis the CSC. The "transparency notice" tool acknowledges and explains this obligation.[10]

4.2 The Four-Step Model

1. Step #1: Personal Data

Data protection law only needs to be taken into consideration if personal data are collected or used. This brings up the following central question in regard to the use of a cloud service:

Are personal data used in the cloud service?

Any information relating to an identified or identifiable natural person ("affected person") is referred to as personal data.

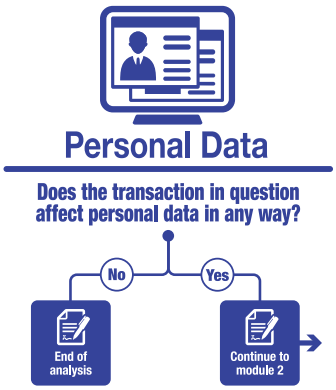
An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

9 The requirements of the individual legal systems are presented in Section V.

10 Section V provides details on the required scope and depth of information.

Examples of personal data:

- IP addresses (as collected by servers in the course of HTTP requests)
- Data on an individual's mobile phone or electricity contract or associated bills (information determining how much the user will be charged)



It is sometimes difficult to assess whether information constitutes personal data.

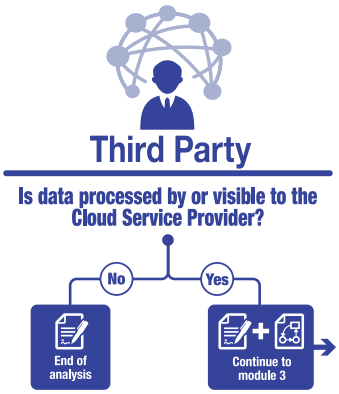
Anonymised information is not within the scope of data protection law. However, researchers have been able to prove that anonymised information can be de-anonymised with enough know-how and the application of enough effort. In any case, the risk of de-anonymisation has increased. In short, the more suited a data set is to de-anonymisation, the more one should assume during analysis that that data set represents personal information.

If the answer is NO, then no data-protection-relevant instruments are required. The cloud service agreement between the CSC and the CSP is sufficient.

If the answer is YES, the second step of the CPC must be executed.

It is important to note that there can be differences between national data protection laws, particularly in regard to the following aspects:

- Are only humans (natural persons) protected by the data protection laws, or are legal persons protected as well?
- When must identifiability be assumed, and what are the requirements for anonymisation?



2. Step #2: Third-Party Involvement

The legal requirement for data protection compliance in the case of the involvement of a third party applies only if the third party has access to personal data.

To what type of access this applies can be regulated differently in the various national data protection laws.

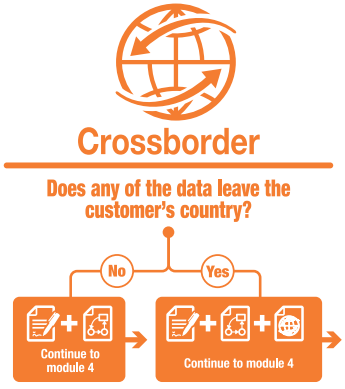
The CPC illustrates when such data-protection-relevant access can generally be assumed not to occur.

The determining factor is the technical design and configuration of the respective cloud service. A so-called transition point can be defined.

If the transition point is not overstepped, the CPC is complete and the cloud service agreement is sufficient.

If the transition point is overstepped, however, a first data protection instrument in the form of a data processing agreement must be instated in addition to the cloud service agreement.

If the answer is YES, then the third step of the CPC must be executed.



3. Step #3: Cross-border Aspects

If the personal data are processed outside of the home country of the CSC, this represents a new dimension in the handling of personal data from a data protection perspective.

The rules for the implementation of the cross-border package of measures differ from country to country. In basic terms, the legal situation can be subsumed as follows:

(1) If the CSP is not affected by any legal system outside of the EU or the EEA, then no further measures are required. In this context, "not affected" means that the CSP neither has its seat or any IT infrastructure outside of the EU/EEA area, nor accesses any data of the CSC from outside of the EU/EEA area.

(2) If the CSP is active in a country outside of the EU/EEA area, but that country is recognized as one with an equivalent level of protection (e.g. Canada, Israel, Switzerland, Uruguay), then no further measures are required.

If the CSP does not fall into the categories (1) or (2), further measures become necessary: either an approach according to the EU standard contractual clauses, or explicit approval.

In its decision of 06/10/2015, the ECJ declared the so-called Safe Harbor principles in their version as per the decision of the EU Commission 2000/520/EC on 26/07/2000 to be invalid. These Safe Harbor principles therefore no longer provide a legal basis for data transfer, and other measures must be taken. Prima facie, the EU standard contract or binding corporate rules are suitable instruments.[11]

If the answer is NO (i.e. there is no cross-border aspect), then no further data protection instrument is required and the fourth step of the CPC is executed.

If the answer is YES (i.e. there is a cross-border aspect), then the "cross-border" package of measures must be activated. Thereafter, the fourth step of the CDC is executed

4. Step #4: Subcontractors

Are any subcontractors involved?

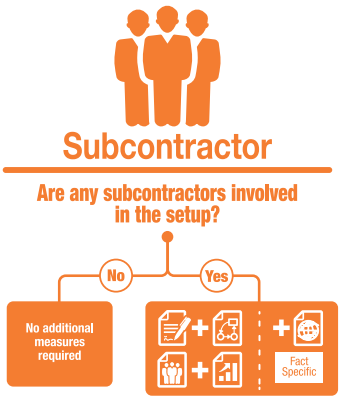
The "subcontractor" package of measures can address the CSC as well as the CSP:

(1) Measures applying to the relations between the CSP and the CSC:

a) Data processing agreement

b) The measures according to step 3 of the CPC are required if the subcontractor has a relevant cross-border aspect.

c) The customer must be sufficiently informed about the involvement of any subcontractor.



(2) Measures applying to the relation between the CSP and the subcontractor: The CSP must pass on his obligations in regard to the data processing to the subcontractor.

(3) Measures applying to the relations between the CSC and the subcontractor: A direct agreement regarding the contracted data processing between the CSC and the subcontractor can improve compliance.

11 According to the statement of the Article 29 data protection group issued on October 16, 2015: "In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, EU-data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used."

Cross-border aspects can influence the analysis in regard to subcontractors:

(1) The implementation of the cross-border package of measures as per step 3 of the CPC should be examined.

(2) The transferral of data can be regulated by way of the EU standard contractual clauses using a subcontractor clause (in Austria, this requires approval by the data protection authority; in Germany, approval is not required; in Switzerland, notification of the authority is sufficient).

It is important to note that EU standard contracts cannot be applied to contract parties which both have their seats within the EU/EEA area. They must be concluded directly between the purchaser within the EU and the contractor in the non-EU/EEA country.

5 Particularities of National Data Protection Laws

The CPC illustrates the four fundamental questions in terms of data protection as regarding the use of cloud services by a CSC and the protection of the CDS. The Legal Toolbox (see Section IV.A) specifies instruments for the data-protection-compliant configuration of cloud usage from the point of view of the CSC.

National differences and particularities can be relevant to the answers given by the CPC. The following section provides a brief overview of these differences for the DACH region (Germany, Austria, and Switzerland).

The sections on the individual countries are arranged according to the four-step model.

5.1 Application of National Data Protection Law

Which laws apply is determined according to the territoriality principle, since each country can only determine the legal norms for its own territory. For the EU member states, this aspect of data protection law is overlaid by an EU directive. The focus of these provisions is always the affected person (CDS). Hence it is not the relation between CSP and CSC that is significant for the determination of applicable data protection laws, but the relation between CSC and CDS.

In simplified terms, the following distinction can therefore be made in terms of the application of data protection law:

- If the CSC has its seat in the same country as the CDS, then the laws of that country apply.
- If the CSC has its seat in an EU/EEA member state and the CDS is located in a different EU member state, then the laws of the country which is the seat of the CSC apply.
- If the CSC has its seat outside of the EU/EEA and the CDS is located in an EU member state, then the laws of the country in which the CDS is located apply.

In order to simplify the terminology used, the following section will consistently use the abbreviation "DPL" whenever national data protection laws are referenced, and the abbreviation "DPA" whenever national data protection authorities are referenced. These abbreviations will be amended by the appropriate two-letter country code. Hence German data protection law will be abbreviated "DPL-DE", and the German data protection authority will be abbreviated "DPA-DE" (and analogously for Austria, "DPL-AT" and "DPA-AT"; for Switzerland, "DPL-CH" and "DPA-CH").

5.2 Austria – Particularities in Data Protection for Cloud Computing

1. General Information

It should be noted at the outset that there currently exists neither a recommendation nor any explicit, consolidated jurisdiction on data protection in Austria in regard to cloud computing. However, the CPC represents a best-practice standard as per DPL-AT. Legally compliant implementation of data protection projects in the area of cloud computing in Austria should therefore likewise be oriented around the **four checks specified in the CPC**:

2. Personal Data

DPL-AT also protects legal persons in regard to information identifying them.

The question whether a personal data aspect remains in the case of pseudonymised or encrypted data is determined by the horizon of the data recipient

3. Involvement of Third Parties

A service provider contracted as an involved third party by the CSC does not represent a third party as defined by DPL-AT. Privileged status due to contracted data processing applies only to service providers whose seat is within the EU/EEA (or in another country considered equivalent).

DPL-AT explicitly requires data secrecy obligations to be extended to the employees of the CSP.

There is no immediate obligation according to DPL-AT to name the involved service provider to the CDS. However, upon request by the CDS, the CSC is obligated to provide the CDS with the name of the involved service provider. Upon request by the CDS, the CSC must also inform the CDS of the location of the data processing.

There is a legal obligation for the CSP to surrender and physically delete the data processed on behalf of the CSC after termination of the data processing agreement. However, there is no legal specification regarding the data format for this surrender.

4. Cross-border Data Transfer

In cross-border data transfer beyond the borders of IT-Schengen, the CSP is authorized to apply for approval by the DPA-AT independently of the CSC if it intends to involve a further subcontractor from another country.

5. Subcontractor Involvement

The CSP may involve subcontractors only with the consent of the CSC. This requires the CSP to inform the CSC prior to involving any subcontractor. Upon request by the CDS, the CSC must provide the CDS with the names of any involved subcontractors. The CSC has the power of veto against the involvement of subcontractors.

5.3 Germany – Particularities in Data Protection for Cloud Computing

1. General Information

German data protection law features particularities which will be discussed in the form of an overview in the following. In-depth information can be found in the "Guideline Cloud Computing: Laws, Data Protection & Compliance" by EuroCloud Deutschland_eco e.V.[12]

Evaluation in terms of data protection law is simplified in Germany by the following document compiled by DPA-DE: "Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises", Version 2.0, dated 09/10/2014 (available only in German). This document will be abbreviated as "Orientierungshilfe" in the following.

The Orientierungshilfe is not a legally binding document, but rather represents an evaluation by DPA-DE. It does not provide dispensation from individual evaluation in regard to data protection law. No court of law is bound to the document in a positive or negative way.

2. Personal Data

DPL-DE protects only natural persons in regard to the information describing them. Legal persons are not protected by default. There is an exception to this principle, however, in the data protection provision of the German Telecommunications Act (GTA). The provisions of the GTA also apply to legal persons, but only in regard to traffic data.

DPL-DE also applies to pseudonymised data, but not to anonymised data. DPA-DE have taken up the position that data protection law must be complied with in the use of cloud services even if the data transferred to the cloud are encrypted in such a way that the CSP cannot correlate them to the respective person. This position is controversial due to its justification, however.

Special regulations apply to so-called "special personal data". According to these regulations, processing of such data in the cloud outside of contracted data processing within the EU or the EEA is not permissible (except, of course, with the explicit consent of the CDS). Special personal data are defined as information on racial and ethnical background, political opinions, religious or philosophical convictions, union affiliation, health or sexual life.

12 *http://www.eurocloud.de/2010/news/datensicherheit/eurocloud-leitfaden-recht-datenschutz-compliance.html*

3. Involvement of Third Parties

A service provider commissioned by the CSC as a contracted data processor as per DPL-DE is not considered a third party according to DPL-DE. However, DPL-DE stipulates the following basic requirements (simplified) for the existence of privileged status:

Careful selection of the CSP by the CSC;

Periodic testing of the CSP by the CSC in regard to IT security;

CSP must be bound to instructions from the CSC;

Data processing agreement as per the requirements of DPL-DE;

Data processing agreement must be in written form.

For all countries not belonging to the EU or the EEA, privileged status does not apply. This is the case even if these countries have been recognized by the EU Commission to provide an adequate level of data protection. This has the following consequences for the evaluation of admissibility of the involvement of third parties:

Within the EU/EEA: Any data processing agreement established correctly in regard to form and content makes the involvement of the third party admissible.

Outside of the EU/EEA: Admissibility in terms of data protection law is to be evaluated by means of a weighing of interests. The existence of a data processing agreement established correctly in regard to form and content positively affects this weighing of interests and hence also the admissibility of the involvement of the third party.

Further requirements must be taken into consideration for cross-border data transfer (see Section 4 below).

In any case, upon request by the CDS, the CSC must disclose to the CDS the name of the service provider and the location of data processing.

The surrender and/or physical deletion of the data processed by the CSP on behalf of the CSC after termination of the data processing agreement must be contractually agreed between the CSC and the CSP.

4. Cross-border Data Transfer

When using a cloud service in a third country, or in the case of personal data being accessed from a third country, further measures must be taken to protect the personal data. These measures are principally the same instruments as those used in other EU member states (e.g. EU standard

contract, individual contracts approved by the respective DPA). Two additional aspects apply in Germany, however:

The use of EU standard contracts requires no notification of, or approval by, DPA-DE. Only individually formulated contracts must be submitted to DPA-DE for approval in order to acquire justificatory effect in terms of data protection law. Special regulations apply to binding corporate rules.

In the opinion of DPA-DE as stated in the Orientierungshilfe, in addition to the abovementioned arrangements, further agreements commensurate with the requirements in terms of content for the data processing agreement must be concluded in any case.

5. Subcontractor Involvement

The subcontractor must be contractually bound by the CSP and made transparent to the CSC in any case. The CSC must also have the possibility of "controlling" the involvement of further subcontractors; i.e. it must at least have the possibility to refuse the involvement of any subcontractor. To this end, any intended subcontractors must be made known to the CSC in due time for it to able to effectively refuse their involvement. The agreement must also grant the CSC the same rights vis-à-vis the subcontractor that it has vis-à-vis the CSP.

5.4 Switzerland – Particularities in Data Protection for Cloud Computing

1. General Information

DPL-CH claims applicability to any transaction relating to affected persons whose residence, seat, or whereabouts are within Switzerland, i.e. the perspective of the affected person is decisive

2. Personal Data

DPL-CH also protects legal persons in regard to the information describing them. DPL-CH defines so-called "personality profiles". A personality profile is a compilation of data allowing evaluation of significant aspects of the personality of a natural person. Personality profiles are coequal to information particularly worthy of protection (sensitive personal data).

DPA-CH treats pseudonymised data as persona data. The legal consequences are determined by a "risk-based approach". DPA-CH has argued against exclusive evaluation from the point of view of the data recipient.

3. Involvement of Third Parties

Privileged status for contracted data processing applies not only in regard to service providers whose seat is within the EU or EEA (or in a third country considered equivalent), but in general

4. Cross-border Data Transfer

Cross-border data transfer justified using approved standard contractual clauses or binding corporate rules must be reported to DPA-CH

5. Subcontractor Involvement

There is no explicit obligation to name involved subcontractors. However, such an obligation can result from the circumstances of individual cases (appropriateness test)

6 Prospect: Draft of an EU-GDPR (EU-GDPR-D)

On 25/01/2012, the EU Commission submitted a first draft for a European General Data Protection Regulation (EU-GDPR-D).

In contrast to the hitherto existing EU data protection regulations, which were issued in the form of directives, the Commission has now chosen the legal form of a regulation. As opposed to a directive, which according to Article 288(c) TFEU requires a national act of transformation for conversion into national law, a regulation is directly enforceable and binding in all member states without the need for an act of transformation according to Article 288(b) TFEU.

In September 2015, the EU-GDPR is still subject to legislative procedures, meaning that its contents have not yet been finalized. The current intent of the EU is for the regulation to be passed sometime during 2016.

The EU-GDPR will become directly enforceable law in all EU member states. It will take precedence over all colliding national data protection regulations except where it defines exceptions. It is currently planned for the EU-GDPR to be applicable only two years after it comes into force. This means that there will be some form of transitional period.

What does the EU-GDPR mean for the CPC? Presumably, the CPC will not need to change at all, for even after the passing of the EU-GDPR, the four fundamental questions will still need to be asked. But their background will then no longer be the respective national legislation, but the EU-GDPR applicable in all member states:

The affectedness of personal data will be decisive for the applicability of the EU-GDPR.

It will be significant in terms of the EU-GDPR whether and how a CSP accesses these data. Contracted data processing and its requirements will also be regulated by the EU-GDPR.

The EU-GDPR will naturally also address cross-border data transfer. Like the national laws in force now, it will stipulate fewer requirements for data transfer within the EU and the EEA as for data transfer to third countries.

And of course the involvement of subcontractors will have to be arranged in accordance with the requirements of contracted data processing, and possible further cross-border transfers taken into consideration.

In summary: The CPC will still be asking the pertinent questions under the new EU-GDPR, and thus remain valid as an instrument for visualisation.

What can the EU-GDPR mean for cloud services:

Standardisation of requirements in terms of data protection law and thus abolition of national particularities e.g. in the evaluation of what information constitutes personal data, or how data transfer into third countries is to be organised.

On the other hand, the EU-GDPR will also impede the coordination of data-protection-relevant positions. For the still data protection authorities will continue to be responsible at a national level and – in simple terms – will have to coordinate with the data protection authorities in other member states in questions with cross-border relevance. This will no doubt be a time-consuming process.

7 Conclusion

The current state of affairs with differing national laws and regulations is unacceptable.

The CPC provides assistance.

Based on these facts, we hereby issue an appeal.

Europe needs a unified and streamlined approach to the cloud.

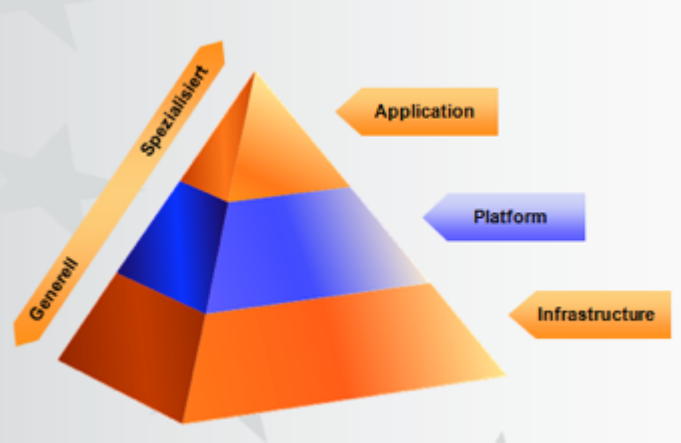
The CPC shows what such an approach might look like.

8 Cloud Computing Glossary

"**Cloud computing** is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Definition: NIST; National Institute of Standards and Technology, USA)

A commonly used basis for illustrating the different elements of cloud computing is the **SPI-Model** which describes the three service levels – Infrastructure, Platform, and Software:

In this model, the three layers are built upon each other, with each layer capable of being used independently of the layers above it.



Public Cloud: IT services are supplied by a cloud provider and can be used by anyone via the internet.

Private Cloud: IT services are supplied via proprietary data centres. All services and the infrastructure are under the control of a single institution. The cloud can be operated by third parties, however. The services are accessed either via the intranet or via VPN (Virtual Private Network).

Hybrid Cloud: A hybrid form consisting of a public cloud and a private cloud.

Federated Cloud: A hybrid cloud with special security features provided by trustworthy service providers in the areas of identification and encryption.

IaaS: Infrastructure as a Service: Provision of computing and storage capacity as a service.

PaaS: Platform as a Service: Provision of "middleware" as a service.

SaaS: Software as a Service: Provision of applications as a service.

XaaS: X as a Service: Provision of additional functions like business processes, networks, communication and others as a service.

9 Legal Information

General

The information provided in this guideline serves the general illustration of certain legal aspects in connection with cloud computing. They do not represent legal advice and cannot replace legal advice, as such advice generally requires knowledge of all individual circumstances, and in particular those of the specific case at hand.

Content of the Guideline

The publisher and the authors assume no liability for the completeness, accuracy or currentness of the information provided. This applies in particular with regard to recent developments in jurisdiction or legislation. Any liability claims against the publishers/authors relating to material or non-material damage of any kind caused by the use or disuse of the information provided, or by the use of incorrect or incomplete information, are explicitly excluded.

References and Links

In regard to direct or indirect references to foreign content (e.g. web links) outside of the responsibility of the publisher/the authors, a liability obligation would arise only if the publisher/the authors had knowledge of the information and were technically able to, and could reasonably be expected to, prevent its use in the case of unlawful contents. The publisher/the authors hereby declare that no unlawful contents were recognizable on the linked webpages at the time of placement of the links. The publisher/the authors have no influence on the current or future design, contents, or authorship of the linked webpages. They explicitly distance themselves from all contents of the linked webpages which were changed after placement of the respective links. Only the offeror of the respective linked webpage is be responsible for any unlawful, incorrect or incomplete contents, and in particular for any damages resulting from the use or disuse of information thus provided, and not the person referencing the webpage by way of web links.

Copyright

The content provided in this guideline, including texts, graphics or images, is protected by Austrian copyright law. Any use not permitted by copyright law requires prior written consent by the publisher. Contributions by third parties are identified as such. This applies in particular to any duplication, editing, processing or reproduction of contents in databases or other

electronic media. Unauthorised duplication or dissemination of the whole or any part of this guideline is explicitly prohibited. Individual and private use is excluded from this prohibition, but private use does not include any right to pass the guideline on to others. The same applies to publications or other documents.

Compensation

This guideline is provided to its addressees/recipients free of charge.

10 Authors

The autors of this guideline are:



Dr. Tobias Höllwarth
EuroCloud Europe
tobias.hoellwarth@eurocloud.org



Dr. Christian Laux
Switzerland
christian.laux@lauxlawyers.ch



Dr. Clemens Thiele
Austria
anwalt.thiele@eurolawyer.at



Dr. Jens Eckhardt
Germany
eckhardt@juconomy.de

EuroCloud AUSTRIA

EUROCLOUD AUSTRIA

VEREIN ZUR FÖRDERUNG
VON CLOUD COMPUTING

MUSEUMSTRASSE 5/14
1070 WIEN, AUSTRIA

E-MAIL: INFO@EUROCLOUD.AT
WEB: HTTP://WWW.EUROCLOUD.AT