TRANSPARENCY, SECURITY, RELIABILITY
TRUST IN CLOUD
www.trustincloud.org
an Initiative of EuroCloud

Cloud Privacy Check (CPC)

Requirements under Data Protection Law that a Cloud Service Customer must ensure when moving into a cloud environment.

EuroCloud

EUROCLOUD AUSTRIA

Cloud Privacy Check (CPC)

Transparency, Security, Reliability – CPC – An Initiative of EuroCloud

Requirements under Data Protection Law that a Cloud Service Customer must ensure when moving into a cloud environment.

Legal Toolbox

STANDARD

- Service Agreement

DATA PROCESSING RELATED

- Data Processing Agreement
- Crossborder Measures
- Subcontractor Measures
- Transparency Notices

1 Personal Data

Does the transaction in question affect personal data in any way?

- No → End of analysis
- Yes → Continue to module 2

'Personal data' is information relating to an identified or identifiable natural person ('data subject'). 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, phsysiological, mental, economic, cultural or social identity.

Examples of Personal Data:
- IP addresses (as collected by servers during HTML requests)
- Data about an individual's phone or electricity account (information that determines how much the individual will be charged)

It is not always easy to assess whether information is Personal Data.

Anonymised information is not within the scope of Data Protection laws. However, researchers were able to prove that anonymised data sets could be de-anonymised by applying enough effort and intelligence. The risk of de-anonymisation has increased. In short, the more a data set is suited to de-anonymisation, the more the analysis must assume the data set is in fact personal data.

2 Third Party

Is data processed by or visible to the Cloud Service Provider?

- No → End of analysis
- Yes → Continue to module 3

Housing *without data access*	SaaS
Zero Out	PaaS
Support *external support no data access*	IaaS
Point of Change	Outsourcing
	Managed *service*
	Hosting
	Support *external support with data access*

3 Crossborder

Does any of the data leave the customer's country?

- No → Continue to module 4
- Yes → Continue to module 4

Crossborder measures vary depending on the country in which the Cloud Service Customer is located. The analysis for Austria, Germany and Switzerland is as follows:

1) If the Cloud Service Provider (CSP) has "nothing" outside the EU/EEA, then no additional measures are required. (In this instance "nothing" means no place of business, no IT infrastructure, and no processes enabling its personnel to access personal data).
2) If the CSP is located in a country which is not part of the EU/EEA, but is ascertained to be in a privileged country (e.g. Canada, Israel, Switzerland and Uruguay) then no additional measures are required.
3) If the CSP does not fall into the categories in (1) or (2), additional measures are needed: EU model clauses; Binding Corporate Rules (BCR's; for group internal processing), or approval (if EU regulations apply, approval is to be issued by the competent authority; under Swiss law, approval is issued by the data subject).

4 Subcontractor

Are any subcontractors involved in the setup?

- No → No additional measures required
- Yes → Fact Specific

Subcontractor measures can be directed at the Cloud Service Customer or at the subcontractor:

1) Commitments of the Cloud Service Provider to the Cloud Service Customer are:
   a) Data Processing Agreement
   b) Compliance Add-On if abroad (see Module #3, Crossborder)
   c) Transparency Notice to the Cloud Service Customer
2) Measure between the Cloud Service Provider and the subcontractor: Agreement imposing the Cloud Service Customer's requirements onto the subcontractor.
3) Measure between the Cloud Service Customer and the subcontractor: A direct data processing agreement can improve compliance.

Crossborder aspects also come into play with respect to subcontractors:

1) Crossborder measures if applicable as per module 3.
2) Onward transfer can be addressed under the EU model clauses with a subprocessor clause or (for group internal processing) under Binding Corporate Rules (BCR's).

Data Protection Exposure

Data Protection Measures

Infographics: Dr. Tobias Höllwarth, Dr. Christian Laux
Content: Dr. Jens Eckhardt, Dr. Christian Laux, Dr. Clemens Thiele

EuroCloud

Design: Jami Rae Dennis

When it comes to moving data into the cloud, data protection rules seem to act as a significant hurdle to cloud customers.

However, the topic of cloud computing and data protection can be consolidated within a few steps. These are summarised in the Cloud Privacy Check, a visualised tool that helps cloud customers find answers faster.

The purpose of the Cloud Privacy Check (CPC) is to determine actions from a data protection perspective on the basis of four simple tests. By applying this method, the legality of using a particular cloud solution can be ascertained quickly and easily, and the appropriate legal action items as required by law can be determined.

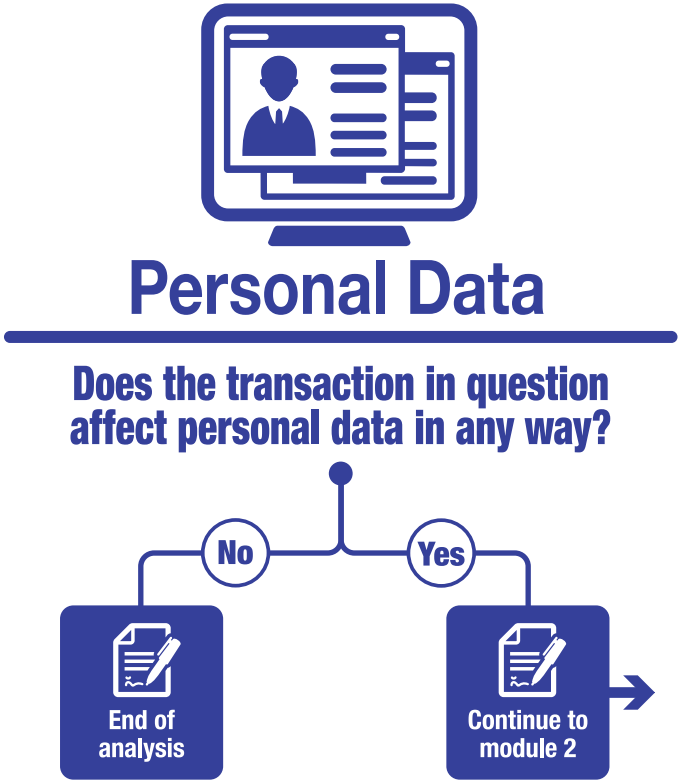
The Cloud Privacy Check is designed to be performed in four test steps. Each step calls for one or more particular action items. The range of the action items that may be needed is presented in the so called CPC Legal Toolbox.

From a data protection perspective, if the action items have been properly implemented, then a cloud solution is deemed to be used in a lawful manner.

In every case, a cloud service contract will be necessary. Further measures may then need to be implemented in order to make the use of a cloud solution compliant from a data protection perspective. We have identified four additional instruments and placed them into what we call the "CPC Legal Toolbox":

1. A Data Processing Agreement.
2. A number of Crossborder Measures, i.e. measures involved when data leaves the country of the Cloud Service Customer.
3. A number of measures in order to make subcontractors part of the cloud computing supply chain.
4. The provision of certain notices to the cloud service customer that help to increase transparency.

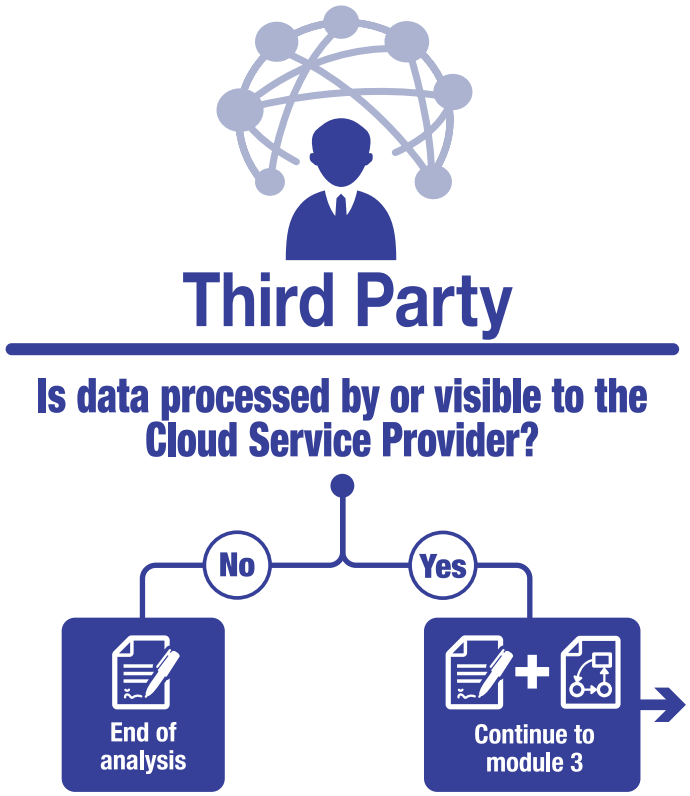
STEP 1 In the first stage of the CPC, we check whether the given fact pattern includes any personally identifiable information.



- If the answer is NO, then no data-protection-related measures are required. The only instrument in place is the service contract between the cloud service provider and the cloud service customer.
- If the answer is YES, the second test of the Cloud Privacy Check must be performed.

STEP 2

In the second stage of the CPC, we check whether a third party - involved within the cloud setup - processes personal data or has access to personal data.



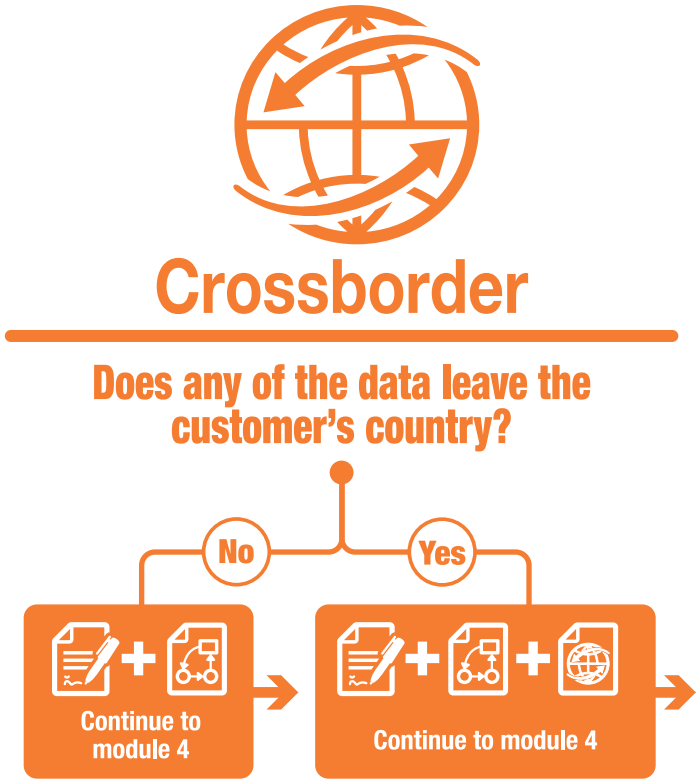
The technical design of the service as provided is crucial. Therefore, a lawyer must analyse and understand the technical setup, i.e. the service design. Within the service design, a point of change can be defined.

- If the point of change is not exceeded, the setup has no specific data protection relevance. The analysis under the CPC can therefore be stopped. The sole instrument in place will be the service agreement between the cloud service customer and the cloud service provider.

- If the delineation marked by the point of change has been exceeded, further controls need to be implemented. In particular, a data processing agreement must be concluded in addition to the service agreement.

After the second stage, the third and fourth tests must be performed.

STEP 3 In stage three of the CPC, we check whether data leaves the home jurisdiction of the cloud service customer.



- If the answer is NO, then no data protection instrument is required as a result of this test, and the analysis can proceed with the fourth test.

- If the answer is YES, then the crossborder „package" must be implemented. This package involves some paperwork (the EU model agreement with the cloud service provider, activation of the Safe Harbor regime, and respective notifications to authorities, if required). After this, the fourth step must be performed.

STEP 4

In the fourth test, we consider whether the cloud provider uses subcontractors.

- If the answer is NO, then the Cloud Privacy Check is complete and no additional instrument needs to be deployed.
- If the answer is YES, the set of measures we refer to as the „subcontractor package“ must be implemented.

  This package requires the cloud service provider to impose the obligations it has - in regard to the cloud service customer - on the subcontractor. In addition, the cloud service customer should be informed of the fact that subcontractors are involved and where they operate. The action item in question here is „Notification of the Cloud Service Customer”. The purpose of this measure is to increase transparency.

  Where data crosses a border while subcontractors are involved, the measures to be deployed can become complicated. We do not address these measures in a comprehensive fashion in the CPC. It is probably easiest to adhere to the EU model clauses (also: „Standard Contractual Clauses“) that cover subprocessing. In some countries, such measures require approval from the data protection authorities (e.g. Austria), while in others it is sufficient to submit a notice to the local data protection authority (e.g. Switzerland).

  Furthermore, a direct data processing agreement between the cloud service customer and the subprocessor can increase compliance.

If the Cloud Privacy Check has been performed in full, you will have the following:

- in the first two steps, you will have analysed whether the setup in question is relevant from a data protection perspective
- in the third and fourth steps, the compliance measures to be undertaken will have become visible.

The CPC process is now complete.

Cloud Privacy Check (CPC)

Transparency, Security, Reliability – CPC – An Initiative of EuroCloud

Requirements under Data Protection Law that a Cloud Service Customer must ensure when moving into a cloud environment.

Legal Toolbox

STANDARD

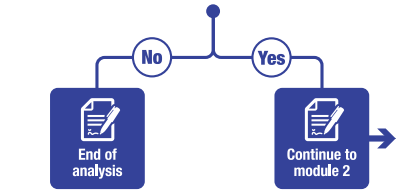
- Service Agreement

DATA PROCESSING RELATED

- Data Processing Agreement
- Crossborder Measures
- Subcontractor Measures
- Transparency Notices

1 Personal Data

Does the transaction in question affect personal data in any way?



'Personal data' is information relating to an identified or identifiable natural person ('data subject'). 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.

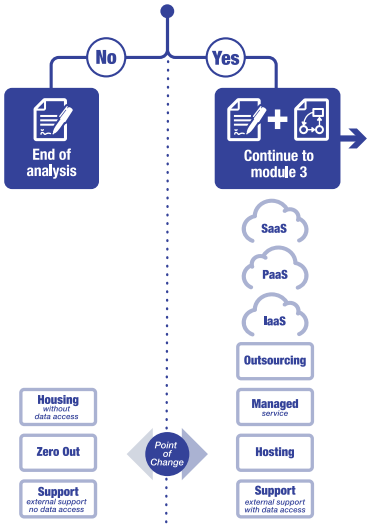
Examples of Personal Data:
- IP addresses (as collected by servers during HTML requests)
- Data about an individual's phone or electricity account (information that determines how much the individual will be charged)

It is not always easy to assess whether information is Personal Data.

Anonymised information is not within the scope of Data Protection laws. However, researchers were able to prove that anonymised data sets could be de-anonymised by applying enough effort and intelligence. The risk of de-anonymisation has increased. In short, the more a data set is suited to de-anonymisation, the more the analysis must assume the data set is in fact personal data.

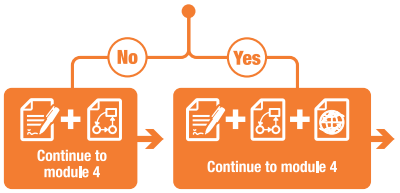
2 Third Party

Is data processed by or visible to the Cloud Service Provider?



3 Crossborder

Does any of the data leave the customer's country?



Crossborder measures vary depending on the country in which the Cloud Service Customer is located. The analysis for Austria, Germany and Switzerland is as follows:

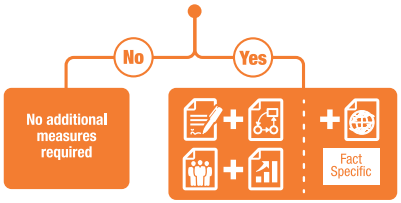
1) If the Cloud Service Provider (CSP) has "nothing" outside the EU/EEA, then no additional measures are required. (In this instance "nothing" means no place of business, no IT infrastructure, and no processes enabling its personnel to access personal data).

2) If the CSP is located in a country which is not part of the EU/EEA, but is ascertained to be in a privileged country (e.g. Canada, Israel, Switzerland and Uruguay) then no additional measures are required.

3) If the CSP does not fall into the categories in (1) or (2), additional measures are needed: EU model clauses; Binding Corporate Rules (BCR's; for group internal processing), or approval (if EU regulations apply, approval is to be issued by the competent authority; under Swiss law, approval is issued by the data subject).

4 Subcontractor

Are any subcontractors involved in the setup?



Subcontractor measures can be directed at the Cloud Service Customer or at the subcontractor:

1) Commitments of the Cloud Service Provider to the Cloud Service Customer are:
   a) Data Processing Agreement
   b) Compliance Add-On if abroad (see Module #3, Crossborder)
   c) Transparency Notice to the Cloud Service Customer

2) Measure between the Cloud Service Provider and the subcontractor: Agreement imposing the Cloud Service Customer's requirements onto the subcontractor.

3) Measure between the Cloud Service Customer and the subcontractor: A direct data processing agreement can improve compliance.

Crossborder aspects also come into play with respect to subcontractors:

1) Crossborder measures if applicable as per module 3.

2) Onward transfer can be addressed under the EU model clauses with a subprocessor clause or (for group internal processing) under Binding Corporate Rules (BCR's).

Data Protection Exposure

Data Protection Measures

Infographics: Dr. Tobias Höllwarth, Dr. Christian Laux
Content: Dr. Jens Eckhardt, Dr. Christian Laux, Dr. Clemens Thiele

EuroCloud

Design: Jami Rae Dennis

CONTACT

Dr. Tobias Höllwarth
EuroCloud Austria
tobias.hoellwarth@eurocloud.at

Dr. Christian Laux
christian.laux@lauxlawyers.ch

Dr. Jens Eckhardt
eckhardt@juconomy.de

Dr. Clemens Thiele
anwalt.thiele@eurolawyer.at