CIO Platform Nederland

CEG Cloud

Essential conditions for the safe use of cloud services

Checklist

Publication of
CEG Cloud & CEG Information Security

CIO Platform Nederland, January 2015, update December 2016

CIO Platform Nederland

CEG Cloud

By the authors

January 2015

All CIO Interest Groups (CIGs) of the CIO Platform Nederland have the goal of sharing knowledge in areas members have indicated as important.

This document contains a concise description of essential conditions for a safe use of cloud services. This is a sort of 'checklist' of conditions to which legislation and / or other common and widely accepted standards can be connected. Organisation specific conditions, and therefore aspects which are more concerned with context are not represented in this overview.

This document is intended as a platform for and an overture for an agreement between Customer and Supplier, in which these aspects are described in detail and officially confirmed.

Evelijn Jeunink (SURFnet), Jacq de Rijck (Coöperatie VGZ), Andres Steijaert (SURFnet), Edwin Strijland (SVB) en Annemarie Vervoordeldonk (SHV).

December 2016

Within the CEG Information Security a check has been done on the Cloud Checklist version January 2015. Purpose is to keep this document up to date.

Changes have been made about Safe Harbour and also new ISO Certifications are listed.

Special thanks go out to Speciale dank gaat naar Arwin Visser (Royal IHC), Andre Gosens (GVB), Frans van der Boom (CZ), Hein Laan (Rabobank), Jean Paul Dijkstra (TBI), Patrick van de Ven (Royal IHC), Stoffel Bos (Prorail) en Norbert Derickx (CIO Platform Nederland).

Table of contents

Applicability Checklist

1.1. Individual

Members of the CIO Platform Nederland can use the overview:

- as a starting point and a reference for supplier contracts;
- when contracting cloud services, by using the description as a point of reference to define good conditions of use.

1.2. Joint

Applying this set of basic conditions as a community of users, united in CIO Platform Nederland, results in:

- a broad basis;
- a common language;

because of which a wider use of cloud services, at the right conditions can be achieved.

This document is an addition to other cloud related documents (published by the CIO Platform Nederland), including the cloud checklist.

Set-up Checklist

Business interests and risk assessment are the main focus when describing the essential conditions for the safe use of cloud services while completing the six focus areas.

A. (Intellectual) property, ownership and control

B. Laws and regulations

C. Security and data integrity

D. Quality and continuity

E. Confidentiality

F. Monitoring and reporting requirements

The following points apply to all elements in the description:

- contracts must be recorded in a written agreement between the Supplier and the Customer;
- they apply to the Supplier, as well as to subcontractors (third parties) whom the Supplier engages in activities. The Supplier is responsible for all subcontractors.

A. (Intellectual) property, ownership and control

1) All (intellectual) property rights of the data (the file or the files) remain at all times with the Customer.

2) The Supplier has no independent control over the data processed by them. Control of the data rests with the Customer.

B. Laws and regulations

1) The Customer is Responsible and the Supplier has the role of Processor.

2) For data export (the transfer of personal data) / international transfer it is assured that data can only be transferred between / within countries or companies which can guarantee an adequate level of protection. The Supplier and the Customer determine the level of protection of the country where the Supplier is located and based on the available level of protection make additional agreements on monitoring and compliance where necessary.

a. For countries of the EU or on the European white list privacy is guaranteed by laws and regulations, and no additional agreements between the Supplier and Customer are required.
b. If the country is not in the EU or is not on the European white list there is no guaranteed adequate level of protection. It is necessary to make agreements by using European model contract clauses, permits (safety net provision) or Binding Corporate Rules approved by the relevant Data Protection Authorities, that describe how a company processes personal data.

3) There may be other applicable laws and regulations, including the Public Records Act, tax laws and regulations, export regulations and eDiscovery.

C. Security and data integrity

1) Suppliers shall take appropriate measures to ensure that the physical and logical security of the Cloud Service is adequately organised against loss or damage and against any form of unauthorised inspection, modification and disclosure or otherwise unauthorised processing of data.

2) If sensitive data: ISO27001 (or derivatives, such as: **BIR and** NEN7510), ISO27015.

3) If privacy sensitive: ISO 27018.

D. Quality and continuity

1) The Supplier is responsible for the quality aspects of the Cloud services and the service level of the Cloud service, in accordance with the agreements made:

a. The Supplier has an escalation and communication plan.
b. The Supplier offers a support clause including priorities in case of calamities.
c. The Supplier and the Customer make agreements on the availability of the Cloud service.

2) The Supplier and the Customer agree on an Exit strategy (in case of termination of service or bankruptcy of the Supplier), in which the following aspects are stated:

a. roles, tasks and responsibilities;
b. the conditions in which the exit strategy enters into force;
c. data portability:
    i. the manner in which it is possible to extract data;
    ii. the manner in which data can be transferred to a different Supplier;
d. the manner in which data should be / is destroyed.

3) The Suppliers shall arrange adequate 'disaster recovery' measures to secure the availability of the Cloud service and thus the availability of the data.

4) The Supplier offers insight into, and the opportunity to give input on, the change- (which changes) and release (when is the change planned) calendar of the Cloud service.

5) The Supplier and the Customer record the exchange standards used in the Cloud service; including the support period of these exchange standards.

E. Confidentiality

1) The Supplier keeps confidential data secret. This means that at least:

a. All data are confidential (which means: should not be made public), unless otherwise indicated.
b. Suppliers will impose a contractual obligation on all those who are involved in the handling of confidential data (including employees) to maintain the confidentiality of this confidential data.
c. The Supplier and the Customer put in writing the consequences of any breach of confidentiality.

F. Monitoring and reporting requirements

1) The Suppliers shall render, at first request from the Customer, all necessary cooperation to exercise supervision by or on behalf of the Customer concerning the use or storage of data by the Supplier.

2) The Supplier shall make all data available to the Customer within the framework of the execution of the agreement (for instance by providing copies) at first request from the Customer.

3) The Supplier shall inform the Customer immediately after becoming aware of a suspected or actual:

i. degradation of the quality (including 'unavailability');
ii. breach of confidentiality;
iii. loss, theft or abuse and / or of confidential and / or personal data; or
iv. breach of security measures;

or when they expect that one of these situations will occur.

Partly so that the Customer is able to comply with the broad reporting requirements, which are part of the Data Breach Notification Bill that currently lies with the House of Representatives in The Netherlands.

4) The Customer is able to carry out periodic audits to test whether the Supplier acts in accordance with the agreements or applicable laws and regulations.

5) The Customer has the right to control the quality and the service level of the Cloud service from a user perspective and shall not be limited by the Supplier.

6) The Supplier shall do their utmost to represent the interests of the Customer during inspections and or orders of authorities by:

a. assessing whether there is a legal obligation to deal with the request or order;
b. objecting to this request or order where possible;
c. not providing more data than required (only providing a minimal data set);
d. informing the Customer as soon as possible.