SCOPE EUROPE

Approval of Declaration of Adherence

Declaring Company: IBM, Declaring Services: IaaS

EU CLOUD COC

Approval-ID	2018PL01SCOPE010
Date of Approval	February 2018
Due date of Approval	February 2019

Table of Contents

1 Approval against v1.7 of EU Cloud CoC (reflecting Directive 95/46/EC)

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 1.7 (**'v1.7'**) as of May 2017.

The EU Cloud CoC v1.7 reflects the Directive 95/46/EC[2]. This version incorporates feedback by the European Commission as well as Working Party 29 given to the version of the EU Cloud CoC as being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**), at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers.

The EU Cloud CoC v1.7 reflects the data protection framework as under Directive 95/46/EC whilst already going beyond – e.g. it requires a continuous, rigorous and independent monitoring of any service adherent.

2 List of declared services

2.1 IBM SoftLayer[4]

IBM SoftLayer provides cloud infrastructure as a service from a growing number of data centers and network points of presence around the world. Products and services include bare metal and virtual servers, networking, turnkey big data solutions, private cloud solutions, and more.

2.2 IBM BlueMix Infrastructure[5]

3 Approval Process - Background

Though being developed against Directive 95/46/EC, the EU Cloud CoC already incorporates continuous, rigorous and independent monitoring. The monitoring is inspired by Articles 40 and 41 European General Data Protection Regulation[6].

3.1 Preliminary Status of the Approval Process

The services concerned passed a preliminary approval process by the Monitoring Body of the EU Cloud CoC, i.e. SCOPE Europe sprl/bvba[7].

---

[1] https://eucoc.cloud
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046
[3] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
[4] http://www.softlayer.com
[5] http://www.ibm.com/bluemix
[6] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[7] https://scope-europe.eu

This preliminary approval process is based on a self-assessment of the service provider completed by a plausibility check performed by the Monitoring Body.

3.2 Safeguards of Compliance

Compliance of adherent services is safeguarded by the interaction of several mechanisms, i.e. continuous, rigorous and independent monitoring, an independent complaints' handling and finally any CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.3 Process in Detail

First the CSP elaborates its corporate and general technical structure and environment with regards of the service(s) concerned to the Monitoring Body. Based on this findings, the Monitoring Body selects a set of qualified questions and determines relevant aspects an initial assessment seems necessary. The plausibility check does not cover all provisions of the EU Cloud CoC at a time. The set of questions qualifies to unfold potential inconsistencies. Such inconsistencies may result into further assessments and questions by the Monitoring Body.

If no inconsistencies were found, declared services are approved and thereupon continuously monitored. The latter safeguards that the full spectrum of EU Cloud CoC's provisions will be assessed within reasonable time.

The CSP may answer either by referencing existing third party audits or certifications and their respective reports or by free text.

The EU Cloud CoC does not provide detailed controls for its single provisions, yet. Therefore it is up to the Monitoring Body to conclude whether the provisions of the EU Cloud CoC are met. Where the EU Cloud CoC provides guidance, the Monitoring Bodies takes such guidance into account accordingly; where no such guidance is provided, the Monitoring Body refers to common interpretations of Directive 95/46/EC especially with regards to court decisions and publicly available documentation on decisions by Data Protection Authorities. Where no such final decision exists the Monitoring Body refers to the common interpretation of Directive 95/46/EC by academics and data protection and information security professionals.

4 Assessment of declared services by IBM (see 2.)

IBM was questioned with regards to multiple aspects of the EU Cloud CoC, including sub-processors, technical organisational measures with regards to security, staff training, contractual transparency, et al.

IBM chose to reach plausibility by both, free text answers and referenced to third party audits and certifications. Furthermore IBM was available for personal meetings and conference calls by which the Monitoring Body could additionally verify the plausibility of information provided by IBM.

IBM answered all questions to the satisfaction of the Monitoring Body, whereas most questions gained plausibility by the according SOC 2 report. **For reasons of transparency:** the provided SOC 2 report is valid until April 2017. It was plausibly declared, though, that there were no substantial changes to the respective aspects and services since.

With regards to sub-processing, the respective services do not incorporate any sub-processors with regards to data; all processing and maintenance is performed by IBM and IBM owned hardware only. **For reasons of transparency:** single hardware may be based in collocation data centres.

With regards to technical organisational measures IBM referred to multiple certifications and audits the services concerned have undergone, i.e. ISO27001, ISO27017, ISO27018, SOC 2, and similar. **For reasons of transparency:** not all data centres are certified and/or audited against all provided certifications and audits. However, provided information gave no valid reasons to raise doubts that there are substantial differences with regards to the overall material level of procedures and technical organisational measures between the different data centres concerned. With regards to the information provided, data centres concerned are subject to identical patterns.

Subject of the assessment were technical organisational measures without focus of individual processing of personal data but with regards to the overall material technical and organisational measures applicable to mere hosting. The customer is responsible for the appropriateness of respective technical and organisation measures with regards to the individual processing due to both the contractual framework and in-line with Directive 95/46/EC. However, IBM provided plausible information that customers may configure their individual set of technical organisational measures required by law; either extending adherent services with additional services or integrating individual measures.

With regards to backups and deletion: deletion, backup and redundancy is subject to the customers' duties. Customers are in full control and may chose the appropriate measures. IBM elaborated its

methods and policies with regards to deletion and confidentiality distinguished between End of Life Management, Server Cancellation and Reclaim, as well as deletion on Mass Storages.

With regards to incident prevention and incident handling and request handling to reveal personal data of customers, IBM provided sufficient information with regards to the technical organisational measures in place to prevent incidents to happen. In the event of an incident a dedicated process is in place to both handle the incident and communicate respective incident to the customers concerned. Respective processes are in place to handle court orders, warrants and requests to reveal personal data of customers. **For reasons of transparency:** The initial assessment of adherence did not scrutinize such processes in detail or if such processes are always followed accordingly; this is up to the continuous monitoring.

With regards to employees, IBM elaborated reasonable processes that deal with both necessary trainings and assessment of employees prior to their access to personal data. **For reasons of transparency:** The initial assessment of adherence did not scrutinize such processes in detail or if such processes are always followed accordingly; this is up to the continuous monitoring.

5 Conclusion

Given answers by IBM were consistent. Where necessary IBM gave additional information or clarified their given information appropriately.

The Monitoring Body therefore approves the services as adherent to the EU Cloud CoC based on plausibility.

6 Validity

This approval is valid for one year.

Approval: Feb. 2018

Valid thru: Feb. 2019

Approval-ID: 2018PL01SCOPE010