SCOPE EUROPE

Approval of Declaration of Adherence

Declaring Company: Epignosis LLC, Declaring Services: eFront

EU CLOUD COC

Approval-ID	2018PL01SCOPE012
Date of Approval	August 15th, 2018
Due date of Approval	August 15th, 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 eFront[4]

eFront is a highly customizable robust Learning Management System (LMS) for enterprises, with unrivaled ease and flexibility, to fit all brand specifications and train masses of employees, partners and customers. eFront is highly secure and can be either hosted in a cloud environment (at a datacenter of a major cloud provider selected by the Customer) or deployed within an organization's intranet. Each Customer administers and manages his own dedicated eFront service instance. Customers can enroll their users and sign them up to the courses ("Learners") created by their Instructors, and customize their LMS by means of specifying custom user roles with certain permissions; using gamification elements; performing a logical separation of their domain into a flat list or a nested hierarchy of different logical units-departments ('Branches'), each with its own courses, learners, instructors and branding (sub-domain, theme, logo) etc. Designed to be the industry's most adaptable enterprise LMS, eFront gives its Customers complete control over their virtual training environment and data. eFront blends seamlessly with any other infrastructure and has the power to grow as the Customer's needs grow.

---

[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] https://www.efrontlearning.com

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[5].

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[6].

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.

---

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[6] https://scope-europe.eu

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 Epignosis (see 2.)

Epignosis 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.

Epignosis chose to reach plausibility by free text answers, only. Furthermore, the Monitoring Body could additionally verify the plausibility of information provided by Epignosis through conference calls.

Epignosis answered all questions to the satisfaction of the Monitoring. Where necessary and appropriate given answers were complemented by graphics as well as references and quotes to internal policies and guidelines. The latter were handed over to the Monitoring Body in full-text and could be assessed, where additional assessment seemed feasible.

Epignosis provides its services engaging sub-processors. Such sub-processors do provide both infrastructure or optional features within the services, such as payment or notification services or document viewer. Epignosis has established an appropriate procedure on engaging sub-processors with regards to both formal aspects (documentation) and substantive aspects (contractual safeguards). **For reasons of transparency:** The assessment did not assess each of the sub-processors individually. However, all sub-processors engaged by Epignosis have been certified at least against one internationally recognized standard like ISO 27001/2, SOC 1/2/3 or PCI-DSS.

With regards to technical organisational measures the assessment focused on the overall approach by Epignosis and whether Epignosis implemented appropriate measures and is capable of reviewing current measures accordingly, and, where necessary, adjust those measures. Epignosis elaborated on both multiple technical measures and internal policies and procedures in place to safeguard personal data processed within their services. **For reasons of transparency:** The initial assessment of adherence did not scrutinize such policies and procedures in detail or if such policies and procedures

are always followed accordingly; this is up to the continuous monitoring; the same applies technical measures.

With regards to incident prevention and incident handling and request handling to reveal personal data of customers, Epignosis provided sufficient information with regards to the technical and 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.

Epignosis implemented a Data Protection Management System (**'DPMS'**) that assigns roles and responsibilities to dedicated positions within Epignosis and establishes policies and procedures that set actions require consultation and / or approval by given roles. Policies and Procedures are frequently reviewed, both by expiry dates and event based. The Data Protection Management System is linked to the respective Management Levels, including top management, Data Protection and IT-Security responsible.

The DPMS incorporates a risk assessment of the personal data processed. Given the contractual framework, services concerned are not intended to process special categories of personal data ('sensitive data') in their default configuration. No matter, all personal data processed is considered as confidential data that comes along with strong technical measures protecting the data processed. Epignosis established policies and procedures to ensure that no sensitive data is processed within its services. On request Epignosis provides individual, hardened configurations of their services to enable customers to address individual risks associated to the personal data processed. **For reasons of transparency:** Subject to the Declaration of Adherence are only services in default configuration. Any individual configurations are not subject to this assessment and will not become subject to any future assessments.

With regards to access control and separation of (customers') data Epignosis provided thorough information on both policies and procedures and technical measures; e.g. employees' access is appropriately limited and logged. Policies extensively require multifactor authorization. Furthermore, services are provided, and data is processed in independent virtual instances for each client. **For reasons of transparency:** The initial assessment of adherence did not scrutinize such processes and technical and organizational measures in detail; this is up to the continuous monitoring.

Epignosis additionally focuses on integrating encryption to all levels as appropriate. Given a full encryption at transit today and a broadly enabled encryption at rest, Epignosis is heading to an enabled encryption in use.

With regards to employees, Epignosis 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

Answers provided by Epignosis were consistent. Where necessary Epignosis 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: August 15th, 2018

Valid thru: August 15th, 2019

Approval-ID: 2018PL01SCOPE012