SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Epignosis LLC, Declaring Services: TalentLMS

EU CLOUD COC

Verification-ID	2020PV02SCOPE002
Date of Verification	January 2020
Due date of Verification	January 2021

Table of Contents

1 Verification against v2.2 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.2 (**'v2.2'**)[2] as of March 2019.

Originally being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC, at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers, the Code was developed against Directive 95/46/EC[4] incorporates feedback by the European Commission as well as Working Party 29. Following an extensive revision of earlier versions of Code and further developing the substance of the Code v2.2 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

The EU Cloud CoC already applies the same principles and procedures now, pending the endorsement of the Code and its official approval by supervisory authorities, cloud service providers are welcomed and invited to sign up their services under v2.2 of the EU Cloud CoC, to publicly underpin their efforts to comply with GDPR requirements.

2 List of declared services

2.1 TalentLMS[6]

TalentLMS is a cloud LMS for businesses of any size to deliver effective and engaging online training to their employees, partners, and customers. Each TalentLMS customer is allocated his own isolated TalentLMS (sub-)domain that is controlled and managed exclusively by him. Customers have full ownership and control of their data and training environment. They can enroll their users and sign them up to the courses ("Learners") created in their domains by their Instructors, and configure and customize their domain. For instance, each Customer may specify custom user roles for his domain with specific permissions. TalentLMS features a robust reporting framework that keeps admins in-the-know. It also offers a list of optional integrations, and capabilities when it comes to customization.[7]

---

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[6] https://www.talentlms.com/
[7] **NOTE**: The content for the service description has been provided by the CSP and does not reflect any opinion of or assessment by the Monitoring Body.

3 Verification Process - Background

V2.2 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[8]. Those mechanisms will apply pending the formal approval of the EU Cloud CoC and accreditation of the Monitoring Body.

3.1 Provisional Status of the Verification Process

The services concerned passed a provisional verification process by the Monitoring Body of the EU Cloud CoC, i.e. SCOPE Europe sprl/bvba[9].

This provisional verification process follows the same principles and procedures as the EU Cloud CoC will apply under its official approval and accreditation. The robust and complex procedures and mechanisms can be reviewed by any third party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[10]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, that has been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue. Unless otherwise provided by the Code, the Monitoring Body's assessment process will be based on an evidence-based conformity assessment, based on interviews and document reviews; pro-actively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body will request additional information. Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

3.3 Multiple 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

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[9] https://scope-europe.eu
[10] https://eucoc.cloud/en/public-register/assessment-procedure/

CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Control's Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third party audits or certifications and their respective reports or by free text. Additionally, the CSP will have to provide a general overview on the functionalities, technical and organizational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognized standards, the Monitoring Body will consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body will verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g. by sample-taking and request for further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g. by media reports, publications and actions of supervisory authorities are covered.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indications for appropriate implementation by the Control Guidance, then the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon make them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.2 of the Code provides three different levels of Compliance. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is however no difference in terms of which parts of the Code are covered since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

3.4.1.1 First Level of Compliance

The CSP has performed an internal audit and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.2 Second Level of Compliance

Additional to the "First Level of Compliance", Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognized standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body will be referred in the Monitoring Body's report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. CSPs must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.3 Third Level of Compliance

Identical to the "Second Level of Compliance" but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognized standards.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[11] and refer to the Public Register of the EU Cloud CoC[12] to enable Customers to verify the validity of adherence.

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

Formally, the assessed services renewed their declaration of adherence, as all of them were declared and verified adherent under the EU Cloud CoC version 1.7. Materially the assessment has been performed as if it was a new declaration of adherence. This result of the fact that v.1.7 of the Code was written against the European Data Protection Directive 95/46/EC, whereas the current version 2.2 was been designed to meet the requirements of Article 40 et seq. GDPR. To adequately address the changes in the requirements of and procedures under the Code, the procedure for new declarations has been applied.

4.1 Fact Finding

Following the declaration of adherence of EPIGNOSIS LLC ('**Epignosis**'), the Monitoring Body provided Epignosis with a template, requesting Epignosis to detail its compliance with each of the Controls of the EU Cloud CoC. Additionally, the Monitoring Body requested an overview and reasoned response on the actual structure of the services declared adherent and why declared services are to be considered a "service family". A service family requires that all services rely on the same core infrastructure, with regard to hardware and software, and are embedded in the same contractual framework.

Epignosis promptly responded to the template also providing additional information to further demonstrate compliance. Information provided for each Control consisted of at least a reference to and / or list of actual measures meeting the requirements of each Control, a free text answer describing their measures, a reference to Epignosis internal controls – where applicable - and a reference to third party audits and certifications, where applicable. This information was complemented by an overview of the actual structure of the service(s) declared adherent, describing the hardware and software and contractual framework, including the use of subprocessors.

[11] https://eucoc.cloud/en/public-register/levels-of-compliance/
[12] https://eucoc.cloud/en/public-register/

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[13], the Monitoring Body analyzed the responses and information provided by Epignosis.

Epignosis declared services are ISO 27001 and ISO 9001 certified. The declaration of adherence referred to the ISO 27001 certification within their responses to Section 6 of the Code (IT-Security). As provided by the Code, the Monitoring Body may consider third party certifications and audits. Accordingly, the Monitoring Body did verify the certification and references. Further in-depth checks were not performed, as provided third party certifications adequately indicated compliance.

A key aspect of the EU Cloud CoC is, also, that Cloud Service Providers have to follow Customers instructions and need to cooperate with Customers in good faith, including possible audits. Declared service(s) by Epignosis are SaaS services. Hence, direct influence of Customers is limited by the type of service being offered, so the Monitoring Body focused on controls related to this key aspect of the Code.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Epignosis which outlined how all of the requirements of the Code were met by Epignosis implemented measures. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of controls from the Code for in-depth scrutiny. The controls selected for this level of review were: 5.1.A, 5.1.E, 5.2.E, 5.2.H, 5.3.B, 5.3.D, 5.4.A, 5.7.A, 5.7.C, 5.8.B, 5.11.A, 5.11.B, 5.11.C.

Additionally, samples were requested regarding Controls: 5.5.A, 5.8.A, Section 6 regarding the Statement of Applicability of the ISO 27001 certification, due diligence regarding APIs that were offered to Customers and measures implemented regarding appropriate separation and access control of Customer Personal Data.

Based on the information provided by Epignosis, a follow-up request was made, for further detail on implemented measures related to Controls and respective information provided for: 5.1.A, 5.1.F, 5.2.H, 5.3.A, 5.3.B, 5.3.D, 5.4.A, 5.8.A, 6.1.B and regarding one common aspect to 5.7.C, 5.8.B, 5.11.A, 5.11.B, 5.11.C.

[13] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

The declared services are very similar as those declared under Verification-ID: 2020PV02SCOPE003. Please refer to the public report[14] and selected controls in there as well.

4.3.2 Findings by the Monitoring Body

During the process of verification, Epignosis consistently gave the impression of having prepared the Declaration of Adherence well and thoroughly. Requests for clarification or additional, supporting information and / or evidence were promptly dealt with and always met the deadlines set by the Monitoring Body.

The Monitoring Body did not focus on Section 6, as current and applicable ISO certifications were provided. The Monitoring Body may rely on such external reports and certifications, if those meet the criteria as set out in the Code, which is indicated where such international audit or certification is already being mapped within the Control's Catalogue. Referenced audits and certifications are those international standards, that have been appropriately mapped to Section 6, so that the Monitoring Body has strong indications allowing the Monitoring Body to rely those. Yet, the Monitoring Body analyzed the certifications and assessed, whether the scope of applicability covered all Controls as provided by the Code, and where Controls were not covered, whether the scope of applicability provided reasons for non-applicability of such controls, that were consistent and convincingly accurate. Epignosis e.g. provided convincing arguments why ISO Control A.6.1.2 does not apply. Nonetheless, Epignosis provided information which measures are implemented that relate to ISO Control A.6.1.2, currently.

Categories of personal data, that might be processed within the service(s) declared adherent, are defined within the Cloud Service Agreement. The categories expected are not directly related to special categories of personal data, though Customers may incorporate such special categories when uploading data sets, which may then indirectly result into the processing of special categories of personal data. Epignosis' services provide a sophisticated level of protection, taking into account the potential risk of provided data, though not explicitly addressing the mere processing of such data. Therefore, the Customer has to ensure that both appropriate consents have been provided and that transparently communicated measures meet the requirements under GDPR. Epignosis supports all data being transmitted into their service(s) via encrypted channels.

The overall impression whilst assessing Epignosis was positive. Epignosis referred to state-of-the-art policies and procedures. Provided samples correspond to the documented policies and procedures

[14] https://eucoc.cloud/en/public-register/list-of-adherent-services.html

and generally met the expectations of the Monitoring Body. Policies and procedures were recently updated, also to meet the requirements of the respective ISO certification. The Monitoring Body invited Epignosis to slightly clarify contractual provisions as well as the applicability and scope of internal procedures. The described intent and scope were consistent with the Code at all times. Anyhow, the actual phrasing might have led to potential misunderstandings of Customers and employee's when applying respective documents. Epignosis instantly implemented any given feedback and thereby demonstrated both its willingness and capability to comply with the Code's requirements. Implemented clarifications even go beyond what Epignosis was invited to, now. **For the avoidance of doubt:** At no time the Monitoring Body discovered any unambiguous breach of neither the Code nor GDPR; Monitoring Body's scrutiny requires to consider even atypical scenarios and non-obvious interpretations, though.

Customers may, always, access diverse information to address their need of transparency and enable them to ensure their own (Customers') compliance with GDPR. Where Customers may adjust implemented measures or may add further (external) services, Epignosis provides background information and manuals assisting Customers to properly decide and configure their services.

Customer data is logically separated, making use of dedicated Customer domains, databases and respective authentication mechanisms. This is complemented by firewalls, subnets and limitation to local requests – where feasible – to add further security.

APIs that are offered to Customers – either by default or as optional connectors – are assessed by Epignosis prior implementation. Compliance with legal frameworks as well as Epignosis quality controls is frequently reviewed. Where such reviews result into any conflicting findings and thus necessary, implementation will be ceased.

5 Conclusion

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

The Monitoring Body therefore verifies the services as compliant with the EU Cloud CoC based on the performed assessment as prescribed in 4. The service(s) will be listed in the Public Register of the EU Cloud CoC[15] alongside this report.

[15] https://eucoc.cloud/en/public-register/

6 Validity

This verification is valid for one year. The full report consists of 11 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify, that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC[16].

Verification-date: January 2020 **Valid thru**: January 2021

Verification-ID: 2020PV02SCOPE002

[16] https://eucoc.cloud/en/public-register/