SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Epignosis LLC

EU CLOUD COC

Verification-ID	2020PV02SCOPE003
Date of Approval	February 2021
Valid until	February 2022

Table of Contents

1 Verification against v2.6 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 2.6 (**'v2.6'**)[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 v2.6 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 v2.6 of the EU Cloud CoC, to publicly underpin their efforts to comply with GDPR requirements.

2 List of declared services

2.1 Merge of all Adherent Services into one Cloud Service Family

As already listed in the previous external reports[6], declared services were already closely aligned so that conclusions of the Monitoring Body could be transferred from one to another, especially related from a technical and internal policy control's perspective. Since the Monitoring Body's last assessment in 2020, Epignosis has continued the alignment process by streamlining its Terms and Conditions as well as Data Protection Addenda . Consequently, all Adherent Services will now be treated as one Cloud Service family.

2.2 TalentLMS[7]

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

[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] Public Report 2020PV02SCOPE002 as of Jan 2020, covering TalentLMS and Public Report 2020PV02SCOPE003 as of Jan 2020, covering TalentCards and eFront.
[7] https://www.talentlms.com/

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.[8]

2.3 TalentCards[9]

TalentCards is a novel micro-learning tool, based on the idea of flashcards but takes its leaps and bounds further. TalentCards is a micro-learning platform that enables businesses to mass-train their people on easily-digestible material. Course administrators create beautiful learning cards in seconds and deliver training over mobile to reach learners anytime, anyplace! TalentCards transforms the learning experience from a mundane and boring process to serious fun. It revolutionizes eLearning by offering mobile users a fun and easy way to learn new information daily on topics of their interest, while leveraging visualization and gamification techniques. TalentCards is ideal for training on safety procedures, compliance, new product knowledge or any other type of training situation that involves bite-sized information. This unique mobile approach offers fast, easy, efficient and fun training, boosting retention and completion rates and enhancing people's knowledge and skills.[10]

2.4 eFront[11]

eFront is a highly customizable robust Learning Management System (LMS) for enterprises. eFront can be either hosted by Epignosis in a cloud environment or deployed within an organization's intranet. Each Customer administers and manages his own dedicated eFront service instance.[12] 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

---

[8] **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.
[9] https://www.talentcards.io/
[10] **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.
[11] https://www.efrontlearning.com/
[12] **NOTE**: Focus of the assessment has been eFront as managed service by Epignosis only. Where Customers maintain their independent instance within their own environment this is out of scope of this assessment. Where the assessment touched areas that may indicate relevance for self-maintained services, this may be – exceptionally – highlighted in the report. In any other case this report must not be used to evaluate any matters related to IT-security or data protection regarding self-maintained eFront instances.

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.[13]

3 Verification Process - Background

V2.6 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[14]. 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[15].

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.[16]

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

[13] **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.
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[15] https://scope-europe.eu
[16] https://eucoc.cloud/en/public-register/assessment-procedure/

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 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

V2.6 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 review 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 specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised 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 shall 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. The CSP 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.

The Monitoring Body may refuse application of Second Level of Compliance if third party certificates and audit reports, that are recognized by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g. the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

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.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

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[17] and refer to the Public Register of the EU Cloud CoC[18] to enable Customers to verify the validity of adherence.

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

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.

[17] https://eucoc.cloud/en/public-register/levels-of-compliance/
[18] https://eucoc.cloud/en/public-register/

Epignosis promptly responded within the template. Information provided consisted of references and list of actual measures meeting the requirements of each Control, a free text answer describing their measures, and a reference to third party audits and certifications, where applicable. Epignosis provided information illustrating the actual structure of their service declared adherent and describing the technical and contractual framework. Epignosis provided the contractual framework for each Service included in the Cloud Service Family.

This assessment has been treated as a renewal. Consequently, the Monitoring Body build upon the experience and fact findings of former assessments.[19] Epignosis confirmed that principally declared Cloud Services were not subject to relevant changes. Updates of the contractual framework as well as modifications to the internal management system and related policies have been transparently communicated to the Monitoring Body allowing the Monitoring Body to perform related assessments if and to the extent considered necessary.

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[20], the Monitoring Body analysed the responses and information provided by Epignosis.

Epignosis declared cloud services subjects to this declaration of adherence[21] have been externally certified and audited, e.g. Epignosis holds current ISO 27001 and ISO 9001 certificates. The declaration of adherence referred to the respective ISO 27001 certification within the 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 indicate compliance.

[19] Public Report 2020PV02SCOPE002 as of Jan 2020, covering TalentLMS and Public Report 2020PV02SCOPE003 as of Jan 2022, covering TalentCards and eFront.
[20] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/
[21] As listed above in section 2.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body requested a completed template where Epignosis elaborates on its implemented measures to adhere to the Codes requirements. As this being a Renewal, the Monitoring Body reviewed Epignosis' responses, checked for completeness and performed a structural and high-level comparison with Epignosis' responses provided in former Declaration(s) of Adherence. Thereby, the Monitoring Body in parallel verified Epignosis statement that no significant adaptations have been performed since its last Declaration of Adherence because the Monitoring Body expects such modifications became evident by performing a high-level comparison.

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.*, 5.4.*, 5.5.*, 5.8.A, Epignosis Standard Operating Procedures

Additionally, samples were requested regarding Controls: 5.1.*, 5.4.*, 5.5.*, 5.8.A, Epignosis Standard Operating Procedures

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.*, Epignosis Standard Operating Procedures

All follow-up responses satisfied the requests made.

For avoidance of doubt: As indicated and explained earlier, the number of follow-up requests do not reflect in any case the quality of service provided, or in any case reflect the quality of compliance of the service.

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. Responses being provided were detailed and never created any impression of intentional non-transparency. Requests for clarification or additional, supporting information and / or evidence were promptly dealt with and always met the deadlines set by the Monitoring Body.

Due to the fact that Epignosis recently updated their Terms of Services, the Monitoring Body focused on related Controls of Section 5.1 of the Code, and a material high-level review of the applicable

updated Cloud Service Agreement. Additionally, the Monitoring Body focussed on verifying the implementation of the provided procedures regarding the management of Subprocessors, Section 5.4 of the Code.

Regarding the assessment of the updated contractual framework, the Monitoring Body needed to verify that also the updated Terms of Services and the Data Processing Addenda (DPA) are compliant with the requirements of the Code. Epignosis confirmed that updates were not materially affecting the contractual framework but principally aligned the framework throughout Epignosis' Cloud Services from a structural perspective. As the contractual framework represents a key aspect of compliance with the Code the Monitoring Body appropriately tested Epignosis' statement that no material (adverse) updates have been performed. For this purpose, various parts of the Terms and Conditions as well as the DPAs were sampled for an in-depth assessments. Particular attention was paid to material differences compared to the versions of the contractual framework subject to previous Declaration(s) of Adherence and, where such differences might be identified, whether these were of relevance from a Code's perspective . The Monitoring Body could not identify any Code-relevant modifications but rather verify that adjustments apply principally to the structure of the contractual framework. Updates of the contractual documents were implemented by Epignosis to its websites during the Renewal process. Monitoring Body verified that updated documents were available to Customers, i.e., the Terms of Services as of September 2nd, 2020 (TalentLMS), December 10th, 2020 (TalentCards and eFront) and according the DPAs as of October 21st, 2020.

Controls related to subprocessing were subject to an in-depth assessment to verify the actual implementation provided procedures regarding the change of subprocessors. As Epignosis reported to have not applied any change of subprocessors since the last Declaration of Adherence, there was no trigger of applicable procedures.

As a current and applicable ISO certification was provided, and 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. The Monitoring Body principally relates to Epignosis' applicable and current ISO certification. Regardless the Monitoring Body will occasionally assess individual Controls of Section 6 of the Code. As Epignosis indicated that Standard Operating Procedures (SOPs) were updated since the last Declaration of Adherence, the Monitoring Body sampled Epignosis' SOPs. Epignosis provided the Monitoring Body with a full set of SOPs. Monitoring Body sampled those SOPs for two purposes: first, verifying no

adverse effects took place, second if Monitoring Body's remarks of prior assessments were considered. Monitoring Body wants to highlight that Epignosis even integrated non-binding remarks, to the extent possible, clarifying or emphasizing data protection related language..

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 1. The service(s) will be listed in the Public Register of the EU Cloud CoC[22] alongside this report.

6 Validity

This verification is valid for one year. The full report consists of 12 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[23].

Verification-date: February 2021 **Valid until**: February 2022

Verification-ID: 2020PV02SCOPE003

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