

Verification of Declaration of Adherence

Declaring Company: Epignosis LLC



EU
CLOUD
COC

Verification-ID 2020LVL02SCOPE003

Date of Approval February 2022

Valid until February 2023

Table of Contents

Verification of Declaration of Adherence	1
1 Verification against v2.11 of the EU Cloud CoC	3
2 List of declared services	3
2.1 TalentLMS	3
2.2 TalentCards	3
2.3 eFront	4
3 Verification Process - Background	4
3.1 Approval of the Code and Accreditation of the Monitoring Body	5
3.2 Principles of the Verification Process	5
3.3 Multiple Safeguards of Compliance	5
3.4 Process in Detail	5
3.4.1 Levels of Compliance	6
3.4.2 Final decision on the applicable Level of Compliance	8
3.5 Transparency about adherence	8
4 Assessment of declared services by Epignosis (see 2.)	8
4.1 Fact Finding	8
4.2 Selection of Controls for in-depth assessment	9
4.3 Examined Controls and related findings by the Monitoring Body	9
4.3.1 Examined Controls	9
4.3.2 Findings by the Monitoring Body	10
5 Validity	11

1 Verification against v2.11 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 2.11 (**'v2.11'**)² as of December 2020.

Originally being drafted by the Cloud Select Industry Group³ (**'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/EC⁴ 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 v2.11 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)⁵.

2 List of declared services

2.1 TalentLMS⁶

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

2.2 TalentCards⁸

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

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.

⁸ <https://www.talentcards.io/>

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.⁹

2.3 eFront¹⁰

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.¹¹ 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.¹²

3 Verification Process - Background

V2.11 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR¹³.

⁹ **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.

¹⁰ <https://www.efrontlearning.com/>

¹¹ **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.

¹² **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.

¹³ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

3.1 Approval of the Code and Accreditation of the Monitoring Body

The services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba¹⁴.

The Code has been officially approved May 2021¹⁵. SCOPE Europe has been officially accredited as Monitoring Body May 2021¹⁶. 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.¹⁷

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 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

¹⁴ <https://scope-europe.eu>

¹⁵ <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf>

¹⁶ <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf>

¹⁷ <https://eucoc.cloud/en/public-register/assessment-procedure/>

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

V2.11 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.

3.4.2 Final decision on the applicable Level of Compliance

When declaring its Cloud Service adherent, the CSP indicates the Level of Compliance it is seeking to achieve. Any final decision, whether a CSP is meeting the requirements of a specific Level of Compliance is up to the sole discretion of the Monitoring Body.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark¹⁸ and refer to the Public Register of the EU Cloud CoC¹⁹ 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.

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.

This assessment has been treated as a renewal. Consequently, the Monitoring Body build upon the experience and fact findings of former assessments.²⁰ 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

¹⁸ <https://eucoc.cloud/en/public-register/levels-of-compliance/>

¹⁹ <https://eucoc.cloud/en/public-register/>

²⁰ [Public Report 2020LVLO2SCOPE003 as of Feb 2021](#), covering the same scope, [Public Report 2020PV02SCOPE002 as of Jan 2020, covering TalentLMS](#) and [Public Report 2020PV02SCOPE003 as of Jan 2022, covering TalentCards and eFront](#).

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 CoC²¹, the Monitoring Body analysed the responses and information provided by Epignosis.

Epignosis declared cloud services subjects to this declaration of adherence²² 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.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from Epignosis which outlined how all 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. In-depth scrutiny reflects sample taking and follow-up questions, whilst the latter may address requests for clarifications or more detailed information.

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.

The controls selected for this level of review were: 5.1.C, 5.1.E, 5.2.D, 5.2.E, 5.2.F, 5.3.D, 5.4.A, 5.4.E, 5.5.D, 6.1.C.

²¹ <https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

²² As listed above in section 2.

4.3.2 Findings by the Monitoring Body

Generally, the Monitoring Body was highly satisfied with the responses by Epignosis. Detailed assessments were mostly related on clarifications.

One focus has been the public communication of Epignosis' adherence to the Code. The publication was principally communicated. The Code was updated since the last assessment, clarifying some aspects on the related requirements. Epignosis' confirmed to implement potentially not fully adapted information accordingly in due time.

Regarding the sub-processing management Epignosis reconfirmed and re-iterated its implemented procedures as assessed in earlier Declarations of Adherence. A dedicated focus was given to the flow-down mechanisms, i.e., whether safeguards provided by Epignosis will also be implemented by any potential sub-subprocessors. Epignosis provided convincing procedures and due diligence towards its subprocessors allowing for an adequate flow-down of the data protection level as provided by Epignosis along the subprocessing chain.

Where Epignosis transfers personal data to third countries, Epignosis relies mainly on the Standard Data Protection Clauses (SDPC), also being called Standard Contractual Clauses (SCC), as published by the European Commission. Where Epignosis may transfer personal data, that require a safeguard under Chapter V GDPR, and which is not safeguarded by the SDPC, Epignosis is aware of any such deviation and thus can react accordingly, in case of need. Epignosis has implemented a continuous monitoring on any changes related to the requirements to adequately safeguard such transfers.

Where Customer may need additional information and evidence, Epignosis provides on the one hand for relevant audit rights to Customers. Additionally, as required by the Code, Customers will also be provided by such information without formally triggering an audit right, but within the general assistance of a Cloud Service Provider towards its Customer, subject to adequate safeguards such as Non-Disclosure-Agreements, where necessary.

To the extent Customers may instruct Epignosis, and those instructions may happen, e.g., by email, Epignosis implemented procedures to ensure that the identity and power of representation for any such instruction are properly verified.

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 CoC²³ alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by Epignosis to support the compliance of its service, the Monitoring Body grants Epignosis with a Second Level of Compliance.

5 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 CoC²⁴.

Verification-date: February 2022

Valid until: February 2023

Verification-ID: 2020LVL02SCOPE003

²³ <https://eucoc.cloud/en/public-register/>

²⁴ <https://eucoc.cloud/en/public-register/>