Verification of Declaration of Adherence

Declaring Company: Epignosis LLC

Verification-ID	2020LVL02SCOPE003
Date of Approval	February 2023
Valid until	February 2024

Table of Contents

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 drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC – at that time called C-SIG Code of Conduct on data protection for Cloud Service Providers – was developed against Directive 95/46/EC[4] and incorporated 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 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]

2.2 TalentCards[8]

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 eFront[10]

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 GDPR[13].

---

[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/bvba[14].

The Code has been officially approved in May 2021[15]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[16]. 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 to 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; proactively 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 process, 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 Controls Catalogue, to the Monitoring Body.

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

With regards to internationally recognised 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 requesting further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided that over a due period every Control will be subject to scrutiny by the Monitoring Body. Where applicable, aspects of current attention at the time of assessment shall be covered too, e.g., where such aspects were indicated in media reports, publications or actions of supervisory authorities.

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 indicating appropriate implementation by the Control Guidance, then, the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon, makes 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 of 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 recognised 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 recognised 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 at 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 Mark[18] and referring to the Public Register of the EU Cloud CoC[19] 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.

As this declaration is a renewal[20], the Monitoring Body requested from Epignosis a confirmation that there has been no material change to the applicable technical, organisational and contractual frameworks. The Monitoring Body also requested from Epignosis a comparison of the declared Cloud Services of last year and this year as well as to explicitly indicate any Cloud Services that are no longer included in the Declaration of Adherence and, where applicable, provide the Monitoring Body with adequate reasons. To the extent the list of Cloud Services was extended, the Monitoring Body requested a confirmation, that any such additional Cloud Services are subject to the same technical, organisational and contractual framework as the original Cloud Services.

---

[18] https://eucoc.cloud/en/public-register/levels-of-compliance/
[19] https://eucoc.cloud/en/public-register/
[20] You can access the Verification Report(s) of previous year(s) via the following link(s): Report 2022

Epignosis promptly responded to the templates. 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 information was completed by the two confirmations requested by the Monitoring Body as well as a detailed comparison of the declared Cloud Services between last year and this year verification highlighting the changes and the reasons for them.

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

Epignosis's declared services have been externally certified and audited. Epignosis holds ISO 27001 certificate, which is valid for the duration of the Declaration of Adherence, and the scope of registration includes all the declared services. The declaration of adherence referred to the relevant 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 verified the certification and references. Further in-depth checks were not performed, as provided third-party certifications adequately indicated 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's 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. The Controls selected for this level of review were: [5.1.A], [5.1.E], [5.2.E], [5.3.B], [5.4.B], [5.5.F], [5.7.D], [5.8.A], [5.9.B], [5.11.C], [5.13.A], [5.14.E], [6.1.C] and [6.2.P].

4.3.2 Findings by the Monitoring Body

During the process of verification, Epignosis consistently prepared the Declaration of Adherence well and thoroughly. Epignosis's responses were detailed and never created any impression of intentional

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

non-transparency. Requests for clarification, additional and supporting information, as well as relevant samples were promptly dealt with and always met the deadlines set by the Monitoring Body.

Related to the Monitoring Body's requests (see section 4.1), Epignosis indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical, organisational and contractual framework. Where additional Cloud Services were added, Epignosis provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

A first area of focus was around data retention. Epignosis, through its Privacy Policy (linked in Epignosis's Terms of Service) indicates that the retention periods of data per situation, i.e., during paid subscription, if subscription is not renewed and if Customer has a free version. Retention policies are enforced automatically in the infrastructure and timelines for subsequent deletion of such data was also confirmed by Epignosis.

The Monitoring Body assessed Epignosis's mechanisms for the transfer of personal data to third countries. Epignosis relies on Adequacy Decisions, which are constantly monitored. In case an Adequacy Decision is voided, the affected agreements are terminated until an alternative mechanism has been officially recognised as being adequate. For transfers to third countries that do not have an Adequacy Decision, Epignosis relies on Standard Contractual Clauses (SCCs) as a safeguard.

Another area of focus was built around subprocessor management. Epignosis has a defined mechanism to notify Customers of changes in subprocessors. The timelines for objection and/or exercising an alternative option, as well as the means to do so were confirmed by Epignosis's contractual documents. For instance, opt-in options are provided to Customers when it comes to optional subprocessors (i.e., non-mandatory infrastructure providers) and Customers can opt out of any optional subprocessors utilising the respective settings from within the platform.

Epignosis's records of processing activities ('ROPA') built another area of focus. Based on the information provided, Epignosis maintains a ROPA in its capacity as Processor, which includes the relevant information as per Article 30.2 GDPR.

Procedures to deal with requests from Supervisory Authorities were assessed. Epignosis's contractual documents confirmed Epignosis's contractual obligations to notify Customers, where legally permissible. In addition to this, Epignosis has an internal procedure to operationalise all privacy requests, including requests from Supervisory Authorities, which includes the steps taken by Epignosis to deal with the respective requests internally and any potential internal escalations.

The Monitoring Body assessed Epignosis's internal timeline for deleting Customer Personal Data after the termination of the Cloud Services Agreement. Epignosis confirmed that such internal timeline would depend on the type of data stored and provided the Monitoring Body with respective timelines.

5 Conclusion

The information provided 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.

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.

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[23].

Verification-date: February 2023 **Valid until**: February 2024

Verification-ID: 2020LVL02SCOPE003

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