SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Fabasoft Cloud

Verification-ID	2021LVL03SCOPE016
Date of Approval	May 2023
Valid until	May 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

Fabasoft Cloud[6] offers Customers the option to save and manage data on the IT infrastructure operated by Fabasoft to use a software product that is integrated into the service. The Cloud Service Fabasoft Cloud is the technical platform for the solutions and products operated in it, such as Fabasoft Business Process Cloud, Fabasoft Approve or Fabasoft Contracts.[7]

As overarching service "Fabasoft Cloud" entails the following products and solutions which were made subject to this declaration of adherence.

- Fabasoft Business Process Cloud
- Fabasoft Approve
- Fabasoft Contracts

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[8].

---

[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://fabasoft.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://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[9].

The Code has been officially approved in May 2021[10]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[11]. 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.[12]

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

[9] https://scope-europe.eu
[10] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[11] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[12] 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[13] and referring to the Public Register of the EU Cloud CoC[14] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of Fabasoft Cloud ('**Fabasoft**'), the Monitoring Body provided Fabasoft with a template, requesting Fabasoft to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration is a renewal[15], the Monitoring Body requested from Fabasoft a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Fabasoft 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

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

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.

Fabasoft 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[16], the Monitoring Body analysed the responses and information provided by Fabasoft.

Fabasoft's declared services have been externally certified and audited. Fabasoft holds an ISO 27001 (including 27018) certificate, which is valid for the duration of the Declaration of Adherence, and the scope of registration includes all the declared services. The third-party audit report referred to the respective ISO 27001 (including 27018) certification within the responses to Section 6 of the Code (IT Security).

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from Fabasoft which outlined how all the requirements of the Code were met by Fabasoft'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.E, 5.1.H, 5.3.D, 5.3.G, 5.7.E, 5.11.A, 5.12.C, 5.12.D.

4.3.2 Findings by the Monitoring Body

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

[16] 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.

Given this declaration of adherence reflects a renewal of a Third Level of Compliance verification, some specifics were necessary to be considered. As with every renewal, the Monitoring Body significantly builds upon its previous findings and ensures that the scope of any renewal contributes to a continuous assessment plan. Given the Third Level of Compliance, the Monitoring Body must ensure, that all relevant findings mainly in Section 5 are not just covered by an existing third-party attestation, but that also the reasons for such third-party to conclude positively can be derived from such attestation. Consequently, the Third Level of Compliance is not incompatible with the Monitoring Body requesting additional information. The Monitoring Body will apply the process that best enables it to conclude on compliance, unless the Monitoring Body was not just validating findings and reasons reflected in the third-party attestation but was gathering key relevant information by itself.

Against this background, the Monitoring Body requested clarifications regarding the existing third-party attestation. The Monitoring Body never had any doubts of compliance by Fabasoft, but need-ed to ensure that the provided documentation is sufficient to allow the Monitoring Body to draw its conclusions.

Where requested, the Monitoring Body received prompt response from Fabasoft and – where needed – from the third-party assessor who drafted the distinct EU Cloud CoC related third-party attestation.

The Monitoring Body focused on how the adherence of Fabasoft has been properly integrated in the existing framework, i.e., that the adherence is adequately communicated as required by the Code and that Fabasoft's personnel is aware of Fabasoft's adherence and may react appropriately if Customers reach out in this respect.

The procedures and policies to respond to requests by supervisory authorities and provide relevant assistance and information to enable Customer to respond to requests by supervisory authorities was in the scope of the assessment. Fabasoft ensures that requests by supervisory authorities are classified as urgent and being dealt by a qualified and dedicated personnel, in due-time and in appropriate detail and quality. The Customer notification mechanism is implemented in line with the EU Cloud CoC requirements. Fabasoft has dedicated Privacy Team to provide necessary support to help Customer to respond to requests by supervisory authorities.

The Monitoring Body has assessed the sub-processor management process. Fabasoft has in place a Purchasing Policy that ensures that data protection obligations and technical and organizational

measures, alongside with other requirements are flow down on the various types of sub-processors. The flow down of the confidentiality obligations are implemented by a signature of the Master Service Agreement or accepting the Fabasoft order by the supplier or service provider. Fabasoft sub-processors can't engage further sub-processors without consent given by Fabasoft. Additionally, Fabasoft reviews the Fabasoft Cloud Service Agreement (including all attachments) to provide reasonable assurance that it contains all applicable elements required under the GDPR, including information about the subprocessors and mechanism to duly notify the Customers of any changes concerning an addition or a replacement of subprocessors, and procedures for the case of the rejection of a subprocessor by the Customer and that these procedures let the Customer exercise termination rights.

Another area of focus was Fabasoft confidentiality obligations with employees and contractors. Fabasoft ensures that relevant agreements containing confidentiality obligations are signed both with employees and contractors, and that such obligations continue after the end of the respective agreements. Fabasoft's employees undergo an obligatory About Fabasoft training that encompasses data protection and information security topics. Moreover, Fabasoft runs an eLearning platform that provides regular courses on information security and data protection, which are obligatory and used to improve security knowledge and awareness and to model appropriate security behaviours to personnel. Such courses are regularly reviewed and their completion are monitored by Fabasoft.

After assessing the provided third-party attestation report and the additional supplementary information received by the assessor upon request, Monitoring Body has no reason to doubt the appropriate performance of the relevant third-party attestation, neither from a formal perspective nor from a material perspective, e.g., that a significantly diverse understanding of the Code has been applied.

Related to the Monitoring Body's requests (see section 4.1), Fabasoft 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, Fabasoft provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

5 Conclusion

The information provided by Fabasoft were consistent. Where necessary, Fabasoft 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[17] alongside this report.

In accordance with sections 3.4.1.3 and 3.4.2 and given the type of information provided by Fabasoft to support the compliance of its service, the Monitoring Body grants Fabasoft with a Third 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[18].

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

Verification-ID: 2021LVL03SCOPE016

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